AIRIS

SRV200 AIRIS Power Server

User's Manual

Table of Content

Introduction....3
Product Specifications....3
Benefits and Key Features....4
Physical Parts and Panel of the Powerful Server....8
Package Contents....10
Quick Installation....11
Hardware Installation....11
Check Your PC First....12
Connect to the Web-Based Manager....14
Web-Based Manager – Basic Settings....16
Configuration Hierarchy....22
Overview of Configuration Menu....23
Network Settings....24
Firewall Settings....31
VPN Settings....35
System Management....37
System Reports....43
User Management....48
NAS Management....50
FTP Server....63
Personal Web Server....65
E-mail Server....66
Windows USB Printer Server....67
Appendix A....70

Introduction

Thank you for purchasing our innovative all-in-one solution---**Powerful Server** appliance for your networking needs.

The AIRIS POWER SERVER integrates server services such as a Network Address Translator (NAT), Virtual Private Network (VPN), SPI firewall, and networked storage into one easy to manage device. The Powerful Server appliance allows a group of trusted computers and networks to connect quickly and safely. With the Powerful Server appliance, network managers and users can save time in establishing some of the most common services done on servers costing thousands of dollars.

Product Specifications

Connection Sharing

- Flexible Address Space for NAT service
- IP Alias
- Multiple NAT

Virtual Private Network

- PPTP Server / Client

Firewall

- Prevent Denial of Service (DoS) Attacks
- Packet/URL Filtering
- Access Control, Virtual Server

System Management

- Web-based Management for Configuring System
- Firmware Update via HTTP
- Reset To Factory Settings
- Event Alert and Logs
- System Information

Services

- DHCP Client/Server
- Proxy DNS
- RIP
- DDNS Client
- FTP Server

Network

- Programmable Static Route
- Network Protocols Supported: PPPoE, TCP, UDP, ICMP, ARP

PPP Authentication

- PAP, CHAP, MS CHAPv2

Real Time Clock

RAID Support

- Supports RAID 0, 1

File Sharing

- Supports CIFS,SMB, AppleTalk(AFP), NFS

User Management

- Local User Account Management

Power Management

- Support Mechanical Off/Soft Off/Sleeping/Working System States

Other Features

- Personal Web Server
- USB Printer Server
- USB Storage Sharing
- Personal POP E-Mail Server

Benefits and Key Features

Virtual Private Network

With Virtual Private Networking, an enterprise can establish a dedicated tunnel among branch offices and/or mobile employees. All data is encrypted and decrypted via the pre-defined dedicated tunnel. This prevents any hackers from stealing private information in the public network. With this

functionality, any sub-network can be grouped as though they are in the same network.

Firewall

The Powerful Server appliance provides a powerful firewall capable of preventing hackers from attacking the gateway or internal network. Many famous DoS attacks can be detected and prevented. Whenever an attack is detected, the system will alert the network manager that an attack has occurred. The network manager can then inspect the log information to find the IP address that sent the packets.

Easy Installation

In order to facilitate the use of the Powerful Server appliance, the product comes with default settings that most network managers can install it without any modification. If the network manager needs to modify any of the settings, the Powerful Server appliance provides an intuitive Web-based user interface.

RAID (Redundant Array of Independent Disks)

RAID is a hard disk access technology that allocates space of disk drives that utilize two or more drives in combination so as to increase fault tolerance and improve overall performance. Powerful Server appliance supports 2 types of RAID, RAID 0 and RAID 1.

- RAID 0 - Striped Disk Array without Fault Tolerance: Provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost. The size of this RAID type equal to sum of Disk 1 and Disk 2.
- RAID 1 - Mirroring Disk Array: A technique in which data is written to two duplicate disks simultaneously. This way if one of the disk drives fails, the system can instantly switch to the other disk without any loss of data. The size of this RAID type equal to single Disk.

Network Attached Storage

Network-attached storage (NAS) is the concept of shared storage on a network. NAS transfers data using industry standard file sharing protocols such as CIFS, AFP, NFS and FTP. Files can be shared simultaneously by clients regardless of the operating system they are using or the network server they are attached to. This solution provides convenient common storage resources.

Dynamic DNS

Dynamic DNS allows anyone wishing to reach your host by the name only. Dynamic DNS will map that name to your current IP address, which changes each time you dial your Internet service provider. With a URL that stays the same all the time regardless of IP address your options become almost as unlimited as a normal content provider like www.indiatimes.com or www.yahoo.com.

USB Print Server

USB Print Server allows any computer in the network to share an USB printer. It complies with USB 2.0 specifications. And the users can print from any computer over a LAN.

Personal Web Server

The Personal Web Server enables users to host an information type website from their appliance. Create your website and place it on the appliance for the world to see. Use it in combination with our built-in DDNS client and anyone with a broadband connection can have their very own website.

Personal POP E-mail Server

The Personal POP E-mail Server provides users the ability to run a personal private e-mail server. Send e-mail you're your registered domain name or just create a DDNS account and have your personalized e-mail address.

FTP Server

FTP is the most secure, fastest, reliable method of transferring files. The FTP server allows you full control over who can login to the Powerful Server appliance, which files the user can access or they could upload data.

Power Management

We divide the power management function into three parts. These are Power

Down and Hard Disk Standby.

We'll describe each part in detail below.

- Power Down

We turn the power down in several ways:

- Power Down by Web

  Please select System Management -> Administrator Settings. In Power Down field, to select the enable radio button and then click the apply button.
- Power Down by press the power button
- Prompt Power Down

  Please press and hold the power button at least 4 seconds.

- Hard Disk Standby

If the hard disk is idle for a while, we would like the hard disk to enter standby mode to reduce the consumption of power. In the left menu, select NAS Management -> RAID Initialization Wizard, in HD Power Management Setting, please select the time in the 'Turn Off hard disk' field (**Figure 1.2**). If you select 'none', the hard disk will not enter the standby mode even if it is always idle. If you select '5 mins', the hard disk will enter standby mode once it is idle for more than five minutes.

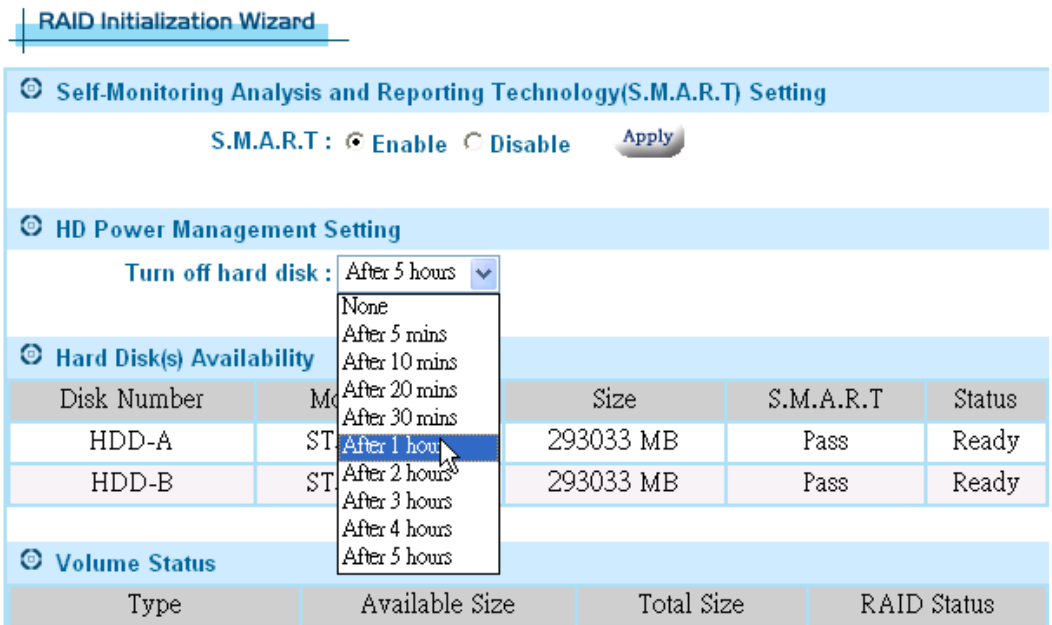


Figure 1.2

Physical Parts and Panel of the Powerful Server

- One WAN port: 10/100 Mbps
- WAN port MDI/MDIX switch
- Four LAN ports: 10/100 Mbps
- Four USB 2.0 port
- Reset Button
- Power Button
- Power Jack - DC 12V
- LEDs: Link/Activity LEDs for Each Ethernet Port, Power LED, HD (Hard Disk) Access LED, HD Indicator & Packet Transmit/Receive LEDs

WAN Port

The WAN port is used to connect to an ADSL/Cable modem for linking to the Internet.

WAN MDI/MDIX Switch

The WAN MDI/MDIX switch is used to adjust the cable connection of the WAN port. If the port is connected to hub, you should move the switch to the “hub” side; if the port is connected to PC like machine, you should move the switch to the “PC” side. As for the four LAN ports, there is no need to add additional switches for each cable connection. This is because the LAN ports support auto MDI/MDIX.

LAN Ports

The LAN ports are used to connect to a PC, server, hub, switch or other network devices on the intranet.

Reset Button

If you forget your password and/or IP settings, you will not be able to access the SA. You can use the **Reset Button** to restore the factory settings. To initiate a reset, you must hold the button for at least 5 seconds.

The primary default settings are listed in the following table.

Configuration Item	Default Settings
Administrator Username	<empty>
Administrator Password	Admin
Internal IP address	172.16.1.1

Power Button

You can use the Power Button to turn on/off Powerful Server.

Description of LEDs

Description of LEDs	Status	Meaning
Power	On	Power On
	Off	Power Off
HD Indicator	On	HD Abnormal
	Off	HD Normal
Access Indicator	Flash	HD is reading/writing data
WAN/LAN Link/Activity	On	Link up
	Off	Link down
	Flash	The interface is transmitting/receiving packets
WAN/LAN 10/100 Mbps	On	The network link is 100 Mbps
	Off	The network link is 10 Mbps
Throughput	No LED on	Current transfer rate is < 10KB/s
	1 LED on	Current transfer rate is > 10KB/s
	2 LEDs on	Current transfer rate is >50KB/s
	3 LEDs on	Current transfer rate is >100KB/s
	4 LEDs on	Current transfer rate is >500KB/s

Package Contents

- Powerful Server
- Power Adapter and Power Cord
- Ethernet cable
- User Manual CD
- Quick Installation Guide

Quick Installation

This chapter will give you brief instructions on how to install the product. In section 2.1, we will configure the hardware part ofAIRIS Power Serverstep by step. In section 2.2, we will check whether the IP address of your PC is assigned by DHCP. Once we complete the installation of theAIRIS Power Serverhardware and checked your PC settings, we will use the web-based management to configure theAIRIS Power Serverto suit your network environment. In section 2.3, and 2.4, we will review all the software settings. We will configure it to gain access to the Internet. If you need additional help or advanced setting details, please refer to the remaining chapters.

Hardware Installation

Please follow the steps below to install hardware:

1. Get the included Ethernet cable.
   Connect one end of it to the ADSL/Cable modem and the other end to the WAN port on the SA.
2. Get another Ethernet cable.
   Connect one end of it to the PC or hub and the other end to one of the LAN ports on the SA.
3. Turn the ADSL/Cable modem on. **Note:** Cable modem users MUST disconnect the cable modem from the wall outlet for at least 2 minutes before turning it on again.
   If there are more PCs or hubs to be connected, please repeat step 2.
4. Connect the included power adapter to the power socket on theAIRIS Power Serverand then plug the power adapter into a wall outlet.
5. Turn on the SA.
   If the link LED of the WAN port is not ON, switch the WAN MDI/MDIX switch to the alternate setting.

The hardware installation is now complete.

Check Your PC First

Please check the following settings on your PC:
Do not assign an IP address to your PC.

1. Please select sequentially: In Start menu -> Settings -> Control panel -> Network connections -> Local Area Connection. Then a “Local Area Connection Status” window shows up. (**Figure 2.2a)**
2. Click the Properties button in Local Area Connection Status. Then the “Local Area Connection Properties” window shows up. (**Figure 2.2b)**
3. Select Internet protocol (TCP/IP) item and then click the Properties button. The “Internet Protocol (TCP/IP) Properties” window shows up. **(Figure 2.2c)**
4. Select the **“Obtain an IP address automatically”** radio button then click the OK button.

Figure 2.2a

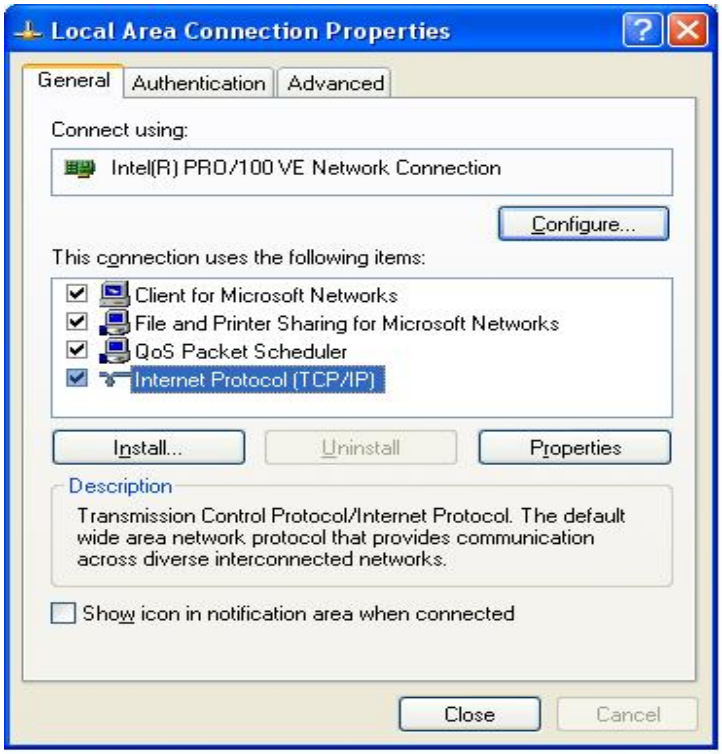


Figure 2.2b

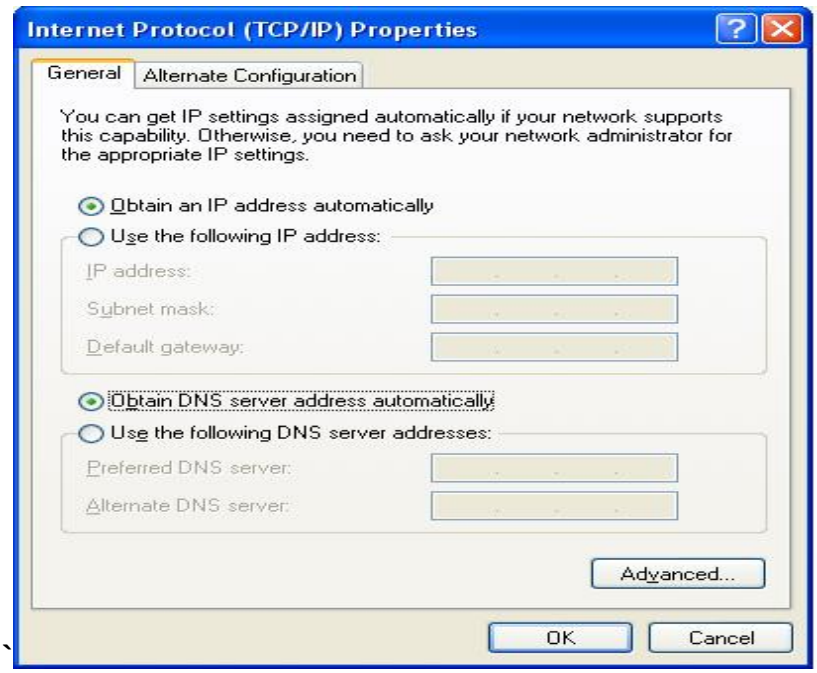
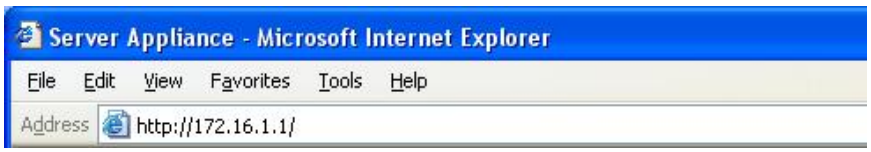

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure 2.2c

Connect to the Web-Based Manager

Please follow the steps to connect to the web-based manager:

1. Open a browser on the PC that is DIRECTLY connected to the SA. Type **“http://172.16.1.1”** in address field. And then press **Enter** key.



2. An authentication window shows up to prompt you to type the username and the password.
3. Leave the username blank and type **“admin”** as a password. (**Figure 2.3a**.)

Figure 2.3a

4. Then press **OK** button. The default web page will appear like **Figure 2.3b**.

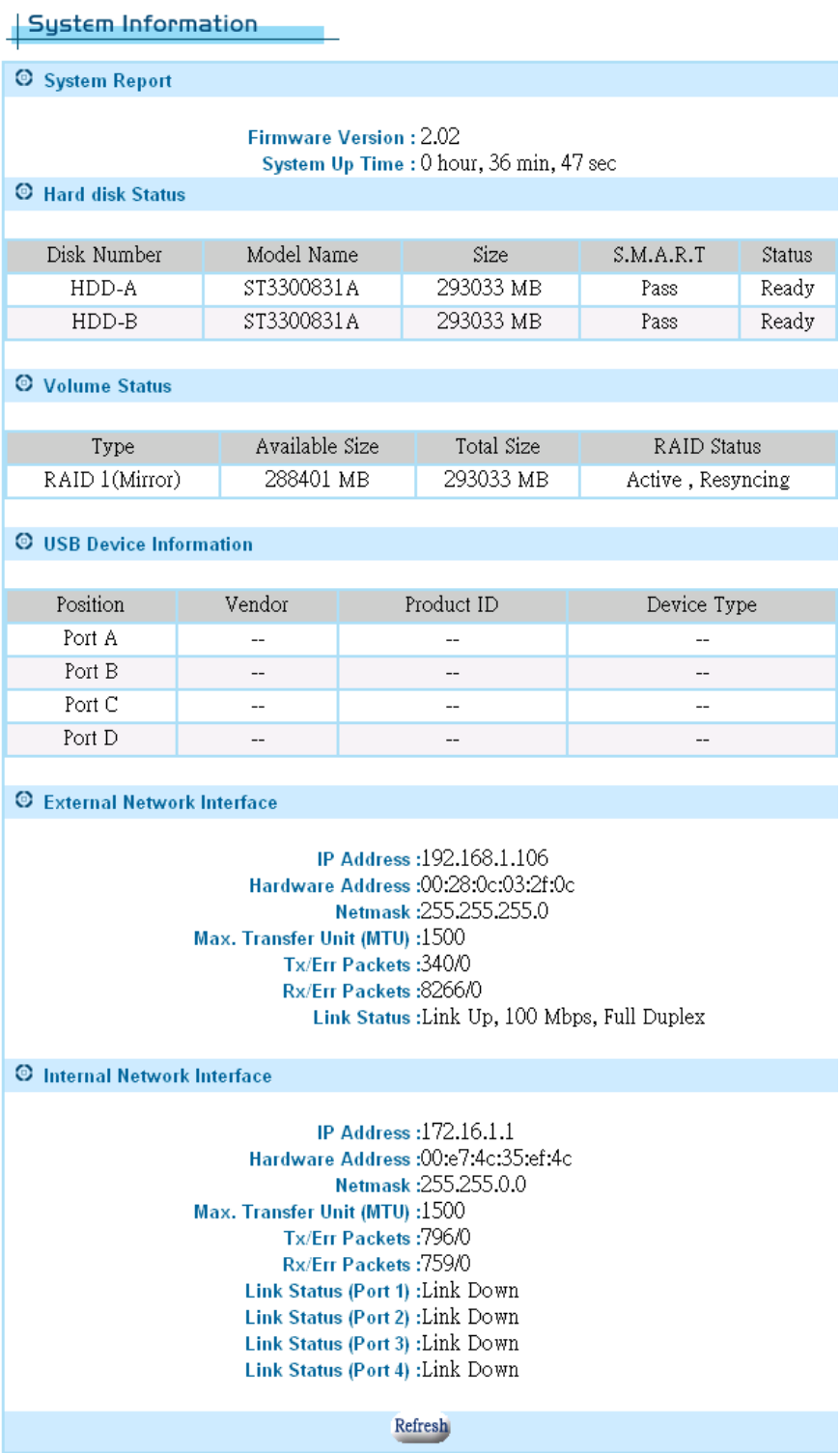

System Information
System Report
Firmware Version : 2.02
System Up Time : 0 hour, 36 min, 47 sec
Hard disk Status
Disk Number | Model Name | Size | S.M.A.R.T | Status
HDD-A | ST3300831A | 293033 MB | Pass | Ready
HDD-B | ST3300831A | 293033 MB | Pass | Ready
Volume Status
Type | Available Size | Total Size | RAID Status
RAID 1(Mirror) | 288401 MB | 293033 MB | Active , Resyncing
USB Device Information
Position | Vendor | Product ID | Device Type
Port A | -- | -- | --
Port B | -- | -- | --
Port C | -- | -- | --
Port D | -- | -- | --
External Network Interface
IP Address :192.168.1.106
Hardware Address :00:28:0c:03:2f:0c
Netmask :255.255.255.0
Max. Transfer Unit (MTU) :1500
Tx/Err Packets :340/0
Rx/Err Packets :8266/0
Link Status :Link Up, 100 Mbps, Full Duplex
Internal Network Interface
IP Address :172.16.1.1
Hardware Address :00:e7:4c:35:ef:4c
Netmask :255.255.0.0
Max. Transfer Unit (MTU) :1500
Tx/Err Packets :796/0
Rx/Err Packets :759/0
Link Status (Port 1) :Link Down
Link Status (Port 2) :Link Down
Link Status (Port 3) :Link Down
Link Status (Port 4) :Link Down
Refresh

Figure 2.3b

Web-Based Manager – Basic Settings

Start to configure your network environment by clicking the **Basic Settings** in left menu. The Basic Settings page is shown as **Figure 2.4a**.

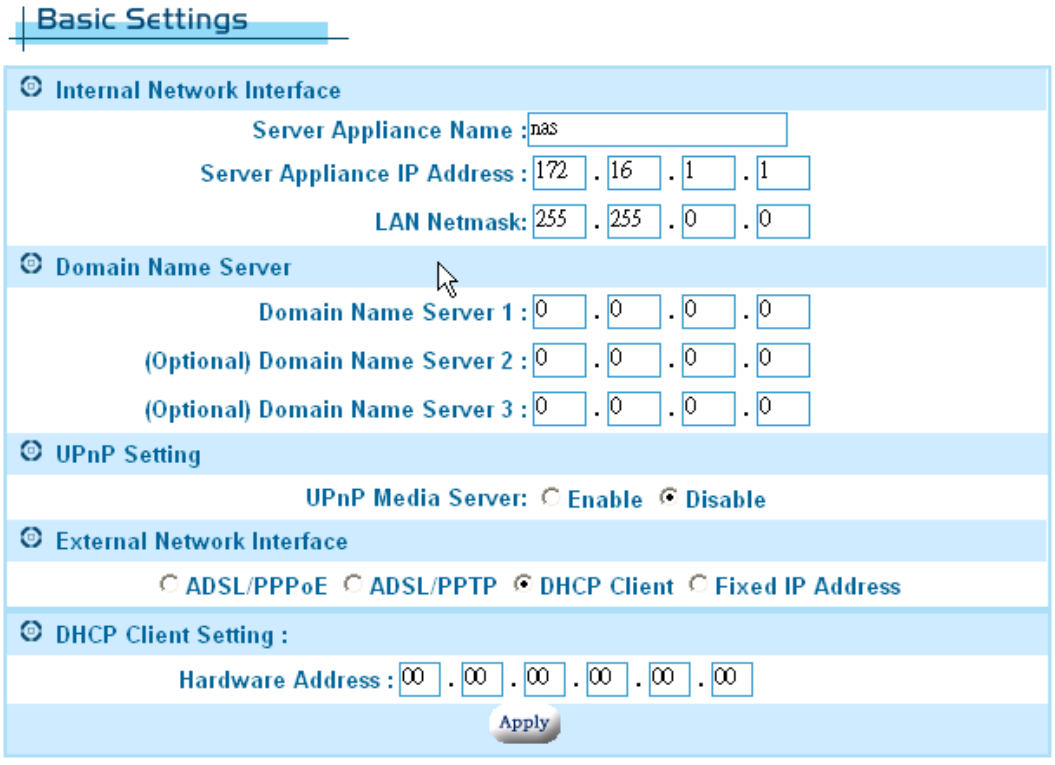

Basic Settings
Internal Network Interface
Server Appliance Name : nas
Server Appliance IP Address : 172 . 16 . 1 . 1
LAN Netmask: 255 . 255 . 0 . 0
Domain Name Server
Domain Name Server 1 : 0 . 0 . 0 . 0
(Optional) Domain Name Server 2 : 0 . 0 . 0 . 0
(Optional) Domain Name Server 3 : 0 . 0 . 0 . 0
UPnP Setting
UPnP Media Server: Enable Disable
External Network Interface
ADSL/PPPoE ADSL/PPTP DHCP Client Fixed IP Address
DHCP Client Setting :
Hardware Address : 00 . 00 . 00 . 00 . 00 . 00
Apply

Figure 2.4a

The Basic Settings page contains **Network Policy**, **Internal Network Interface**, **Domain Name Server**, and **External Network Interface**. We describe these settings below in detail. You must click the apply button after you finish inputting the settings. You will see a rebooting window as **Figure 2.4b**. During the rebooting phase, do not turn off or unplug the Powerful Server appliance.

Figure 2.4b

·Internal Network Interface

The default settings are:

- Host Name: “SA”
- Private IP: “172.16.1.1”
- Private IP Netmask: “255.255.0.0”

According to the default settings, we will assign the LAN to network “172.16.1.x” You can add more detailed configurations later in section 4.1 DHCP Server settings.

For the Network Address Translation (NAT) application, the private network address should be set in the following address range reserved by the Internet Assigned Numbers Authority (IANA).

Class	Address Range
A Class	10.0.0.0/10.255.255.255
B Class	172.16.0.0/172.31.255.255
C Class	192.168.0.0/192.168.255.255

Domain Name Server

- Most of the time this information is not needed, as your ISP will automatically provide the information.
- Please ask the DNS IP address from your ISP if one is required.

External Network Interface

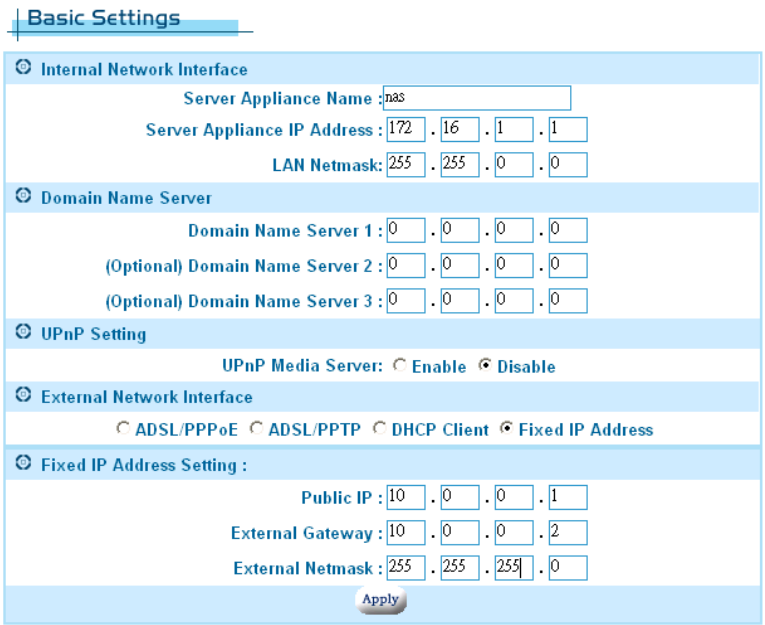
External network interface includes **ADSL/PPPoE** , **DHCP Client** and **Fixed IP Address** settings. Make sure that the system information webpage shows that your Link status is 'Link Up'. If not, please check your connection and/or switch the MDX switch located next to your WAN port. We have to choose one of the three ways to configure the external network interface. They are illustrated as follows:

Example 1: If you are connecting through a fixed IP address from the ISP.

Example 2: If you are connecting through a dynamic IP address from ISP.

Example 3: If you usually enter a username and password to access the Internet.

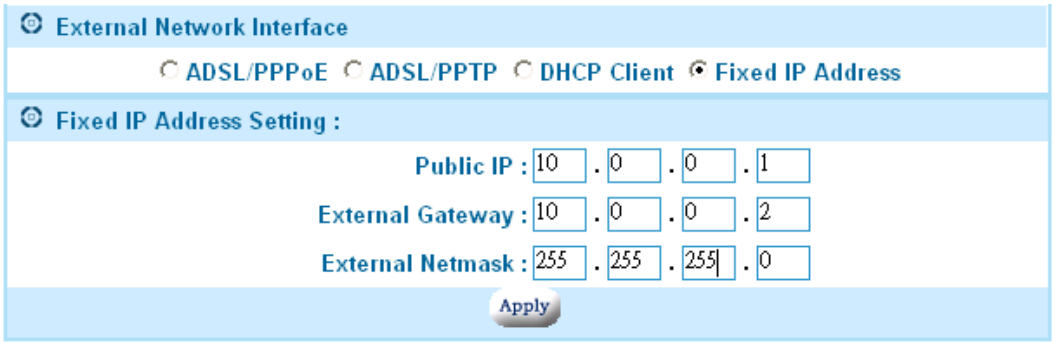
Example 1: Fixed IP Address Settings


Basic Settings
Internal Network Interface
Server Appliance Name : nas
Server Appliance IP Address : 172 . 16 . 1 . 1
LAN Netmask: 255 . 255 . 0 . 0
Domain Name Server
Domain Name Server 1 : 0 . 0 . 0 . 0
(Optional) Domain Name Server 2 : 0 . 0 . 0 . 0
(Optional) Domain Name Server 3 : 0 . 0 . 0 . 0
UPnP Setting
UPnP Media Server: Enable Disable
External Network Interface
ADSL/PPPoE ADSL/PPTP DHCP Client Fixed IP Address
Fixed IP Address Setting :
Public IP : 10 . 0 . 0 . 1
External Gateway : 10 . 0 . 0 . 2
External Netmask : 255 . 255 . 255 . 0
Apply

If you have a fixed IP address from your ISP to access the Internet, please follow the steps below:

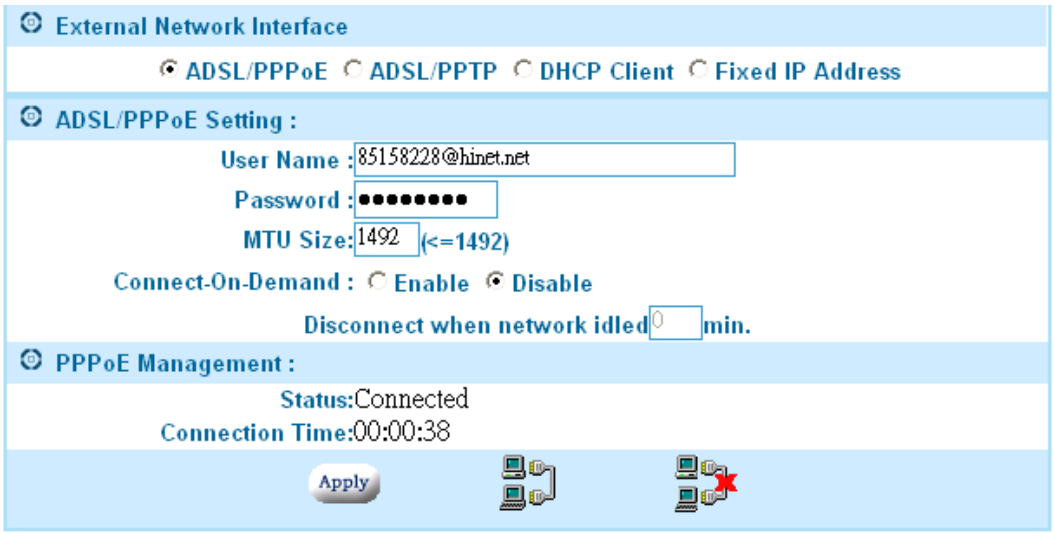
1. Select the **Fixed IP Address** radio button.
2. Enter the Public IP address.
3. Enter the External Gateway.
4. Enter the External Netmask.
5. Click the apply button.

Example 2: DHCP Client / Cable Modem


External Network Interface
ADSL/PPPoE
ADSL/PPTP
DHCP Client
Fixed IP Address
Fixed IP Address Setting :
Public IP : 10 . 0 . 0 . 1
External Gateway : 10 . 0 . 0 . 2
External Netmask : 255 . 255 . 255 . 0
Apply

If you have a dynamic IP address from your ISP to access the Internet, please select the **DHCP Client radio** button. Once the external IP address is obtained via the DHCP protocol, there is no need to give an external IP address, external gateway address or netmask. The DHCP server will dynamically assign these fields. In general, you should choose this option if you are connecting the Powerful Server appliance to a cable modem. **Note:** Cable modem users MUST disconnect the cable modem from the wall outlet for at least 2 minutes before turning it on again. Some cable modem connections need you to provide specific hardware address. For the case, you should fill your hardware address that you get from your ISP provider in Hardware Address field to override the original hardware address. However, it does not update the original hardware address stored in EEPROM. If you would not like to override the hardware address, you should set each field of the **Hardware Address** to zero “00”.

Example 3: ADSL Connection



Most ADSL connections do not give you a fixed IP address. In this case, you must enter the user name and password provided by your ISP for authentication. Please follow the steps below.

1. Please select the **ADSL/PPPoE** radio button.
2. In **ADSL/PPPoE Setting**: Enter the **User Name** and **Password**.
3. Click the apply button to save your settings.

After completing your configuration, each time theAIRIS Power Serverboots, it will try to connect with your ISP and the ISP will assign the Powerful Server appliance an external IP address. Once successfully connected, the Status field should reflect this. If the Status is still the same, check to make sure that the username, password, cables, etc. are all correct.

Example 4: ADSL/PPTP Client Setting

If your ISP provides a PPTP server, you could set up the PPTP client here.

Please follow the steps:

1. Select ADSL/PPTP radio button.
2. Enter the user name. (You get this from your ISP)
3. Enter the password. (You get this from your ISP)
4. Enter the IP address of your host in My IP Address.
5. Enter the IP address of the server in Server IP Address.

In the following chapters, we will cover more details of configuring the SA.

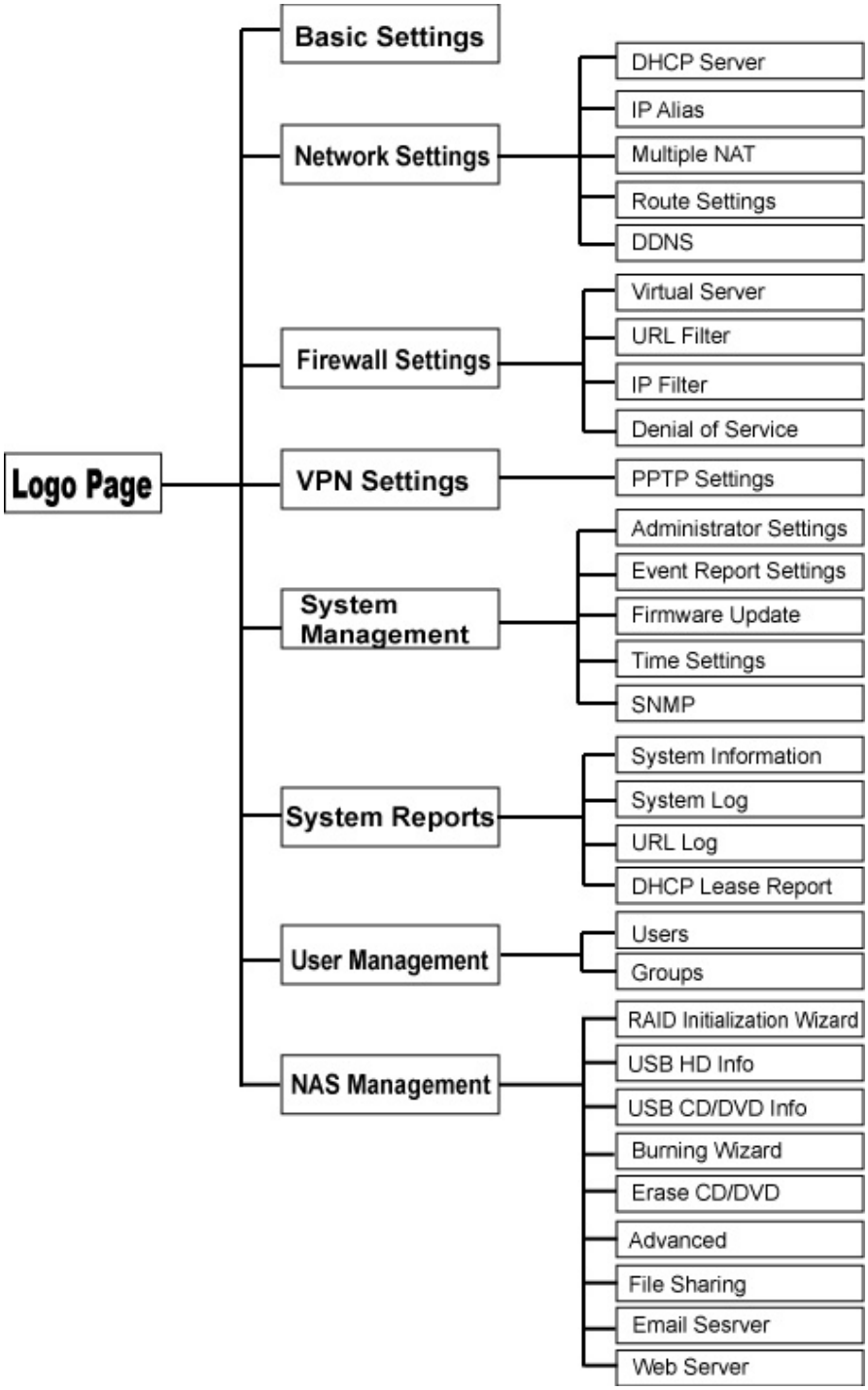
Configuration Hierarchy

This chapter gives you an overview of all the configuration options available. The Powerful Server appliance is a multifunction product. The section3.1 explains the corresponding settings for each function. And in section3.2, we describe the power management in detail.

There are eight main categories in configuration menu, **Basic settings, Network settings, Firewall settings, VPN settings, System management, System reports, User management and NAS management**. Each item has advanced configurations. See **Figure 3.1.**

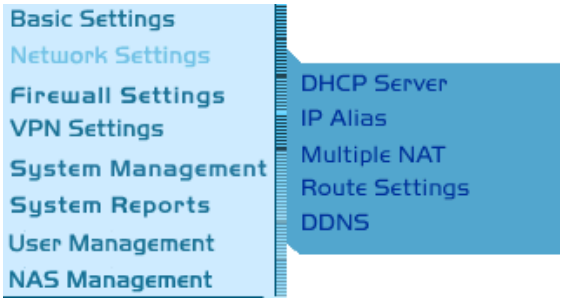
Overview of Configuration Menu

Figure 3.1

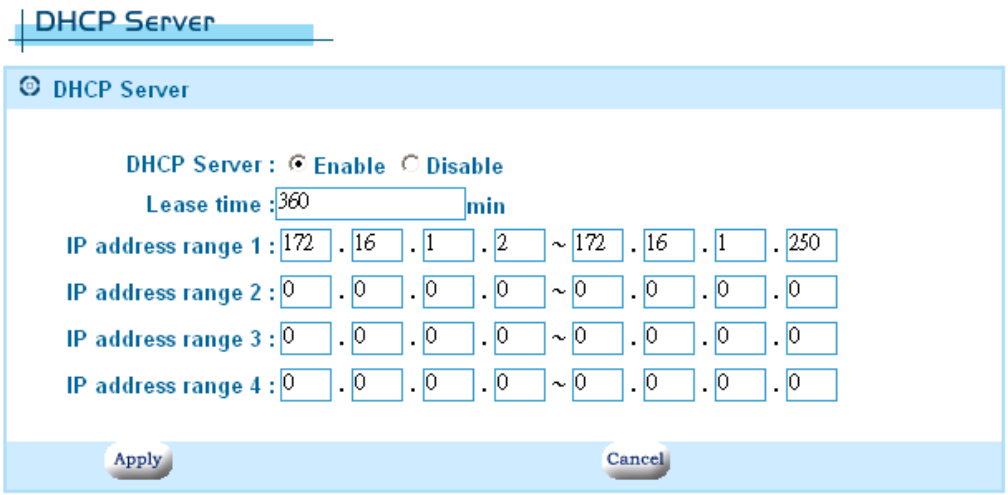


Network Settings

When you select Network Settings in the left menu of the web page, five configuration options appear: DHCP Server, IP Alias, Multiple NAT, Route Settings and DDNS. Please refer to the corresponding section for these configurations.



DHCP Server


DHCP Server
DHCP Server
DHCP Server : Enable Disable
Lease time : 360 min
IP address range 1 : 172 . 16 . 1 . 2 ~ 172 . 16 . 1 . 250
IP address range 2 : 0 . 0 . 0 . 0 ~ 0 . 0 . 0 . 0
IP address range 3 : 0 . 0 . 0 . 0 ~ 0 . 0 . 0 . 0
IP address range 4 : 0 . 0 . 0 . 0 ~ 0 . 0 . 0 . 0
Apply
Cancel

In DHCP Server settings, we assign the rage of the virtual IP addresses for the four LAN ports of SA. All devices connect to the LAN ports ofAIRIS Power Serverwill be dynamically assigned the IP addresses within the range. If you wish to **mix dynamic and static IP clients** on your network: Under DHCP server settings, theAIRIS Power Serverdefaults to assigning IPs 172.16.1.2 through 172.16.1.250...So depending on how many fixed IP devices they have, they can assign their device to an IP of 172.16.1.251 (through 254) as these IPs will not be handed out by the SA.

If they have more devices or want a different IP range, then all they need to do is modify the range that theAIRIS Power Serverhands out so it does not hand out an IP in that range. Typical offices set their DHCP server to assign IPs from 30 through 200. IPs 1 through 29 are usually assigned to servers and 201 and above are reserved for special uses.

You can either enable the DHCP server or disable it in this screen also.

- **To Enable the DHCP Server**

If you do not have a DHCP server on your network,

1. Select the **Enable** radio button.(already enabled by default).
2. Enter a number in Lease time field.
3. Enter the IP address range1 as “192.168.0.2” and “192.168.0.250” (default).
4. Enter the IP address range2, otherwise enter “0” in each field.
5. Enter the IP address range3, otherwise enter “0” in each field.
6. Enter the IP address range4, otherwise enter “0” in each field.
7. Click the apply button.

When DHCP server is enabled, it will allow DHCP clients to obtain their network configuration from the unit. In the figure above, the IP address range of 192.168.0.2 to 192.168.0.250 is dynamically assigned to individual DHCP clients. The DHCP client may be assigned an IP address like “192.168.0.10”. The IP address “192.168.0.1” cannot be assigned as it is not in the range and is also assigned toAIRIS Power Serverunder Basic Settings. If you assign another network (e.g. 192.168.1.x) to IP address ranges 2, 3, 4, please refer to section 4.2 for further **IP Alias** setting. When no other IP address ranges are assigned, a zero value should be filled in to indicate that no other IP addresses are available for assignment.

- **To Disable the DHCP Server**

  If you already have a DHCP server on your network,

  1. Select **Disable** radio button
  2. Click the apply button.

- **Or you do not have DHCP server on your network, but you would like to assign a static IP address to each device**

connected to the LAN port of SA.

1. Select **Disable** radio button.
2. Assign a static IP address to each device connected to the LAN port.

For example, you have four PCs, PC1, PC2, PC3 and PC4 connected to the LAN port. You have to assign a UNIQUE static IP address i.e. “192.168.0.34”, “192.168.0.25”, “192.168.0.18”, “192.168.0.108” to PC1, PC2, PC3 and PC4 respectively. **Note:** The **static IP addresses** assigned are all in the same subnet with SA. In Basic Settings, we set “192.168.0.1” as private IP address ofAIRIS Power Serverwith a 255.255.255.0 subnet. Therefore, the networked PCs need to belong to “192.168.0.x”.

IP Alias

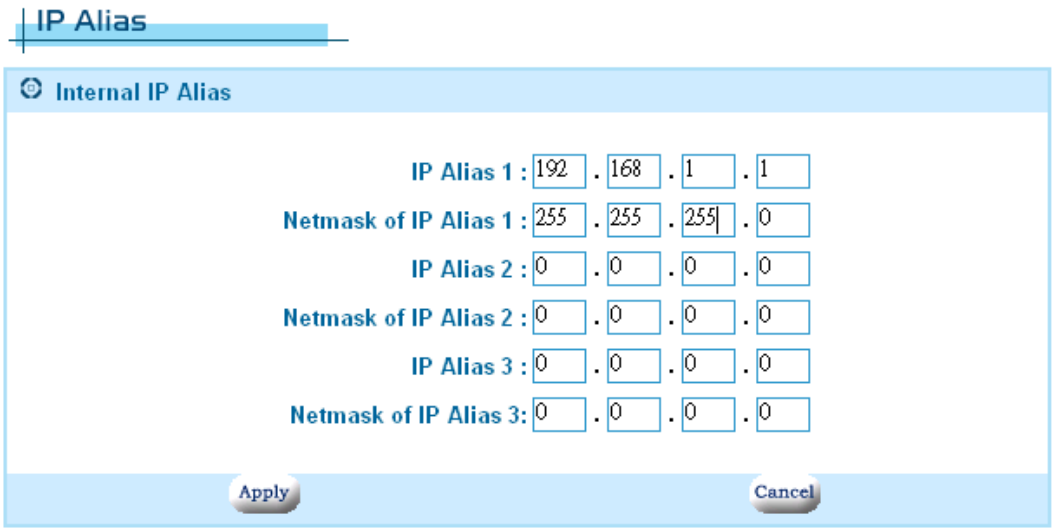
In Basic Settings, we’ve set the private IP address ofAIRIS Power Serveras “192.168.0.1”. We will assign the LAN ports ofAIRIS Power Serverto the network of “192.168.0.x”. In DHCP server settings, we’ve set the IP addresses of the LAN as “192.168.0.x”. “192.168.0.x” includes “192.168.0.x”, and therefore is considered to be in the same network. There is no problem if the network interface contains only one IP address range, but if you want to assign another IP addresses like “192.168.1.x” to the LAN, then there is an issue. “192.168.1.x” and “192.168.0.x” are not in the same network. We need IP Aliasing to resolve this issue. IP alias allows one network interface to contain more than one network. It allows the additional network “192.168.1.x” to be recognized by the SA.

Please follow the steps to add another network:

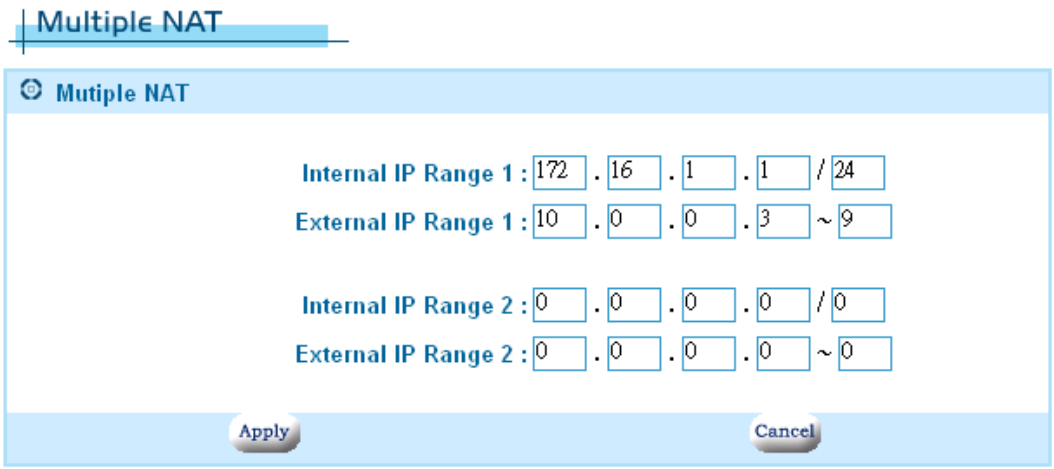
1. Enter “192.168.1.1” in IP Alias 1.
2. Enter “255.255.255.0” in Netmask of IP Alias 1.
3. Click the apply button.

Note that the **IP Alias 1**, **192.168.1.1** is assigned toAIRIS Power Serverand the network is “192.168.1.x”.

For additional IP addresses of the internal network interface to be accepted, enter the other IP address in IP Alias 2 and IP Alias 3. Enter “0” in each field if none.


IP Alias
Internal IP Alias
IP Alias 1 : 192 . 168 . 1 . 1
Netmask of IP Alias 1 : 255 . 255 . 255 . 0
IP Alias 2 : 0 . 0 . 0 . 0
Netmask of IP Alias 2 : 0 . 0 . 0 . 0
IP Alias 3 : 0 . 0 . 0 . 0
Netmask of IP Alias 3: 0 . 0 . 0 . 0
Apply
Cancel

Multiple NAT


Multiple NAT
Mutiple NAT
Internal IP Range 1 : 172 . 16 . 1 . 1 / 24
External IP Range 1 : 10 . 0 . 0 . 3 ~ 9
Internal IP Range 2 : 0 . 0 . 0 . 0 / 0
External IP Range 2 : 0 . 0 . 0 . 0 ~ 0
Apply
Cancel

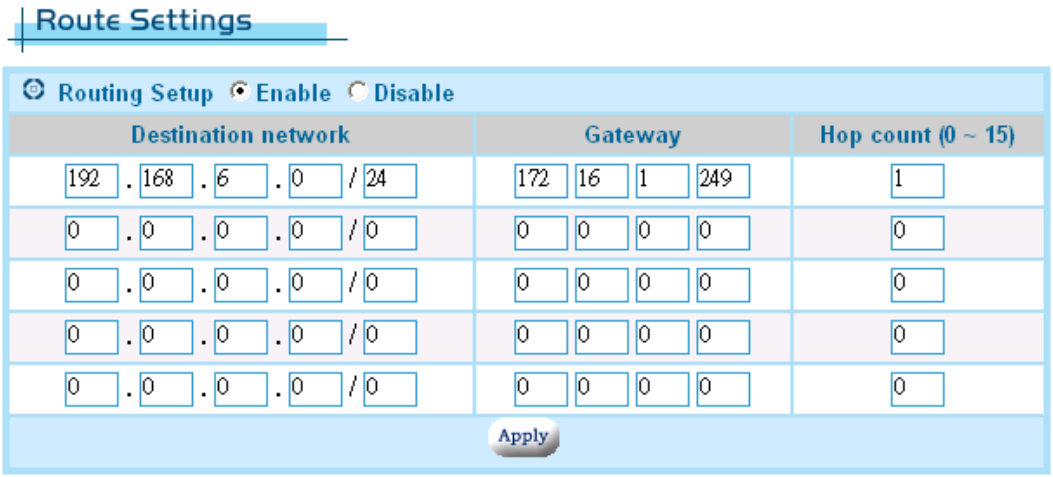
If you get several fixed IP addresses from your ISP and the ISP restricts the bandwidth for each fixed IP address, you have to prevent the network packets from always sending on the same IP address and the other IP address to sit idle. Multiple NAT solves this and allows you to increase the bandwidth. Multiple NAT allows you to dispatch your network packets evenly to these IP addresses provided by ISP.

1. Enter the Internal IP range1, e.g. “172.16.1.1/24”. It means the network is “172.16.1.x”
2. Enter the External IP range1, the IP address range you get from your ISP.

3. Enter the Internal IP range2, e.g. “192.168.1.1/24”. It means the network is “192.168.1.x”.
4. Enter the External IP range2, the IP address range you get from your ISP.
5. Or enter “0” in each field for non-setting multiple NAT.
6. Click the apply button.

After you configure the Multiple NAT on the group of fixed IP addresses, it can increase the bandwidth. The Internal IP range you entered will be routed to the corresponding External IP range.

Route Settings



The Route Settings page gives you a way to set the static route. You have to set the static route if you would like to route your packets to the specific network and the router of the destination network does not support RIP (Routing Information Protocol). If the router supports RIP, it will automatically exchange routing information withAIRIS Power Serverand it is not necessary to set a static route. Please refer the steps and figures to set a static route.

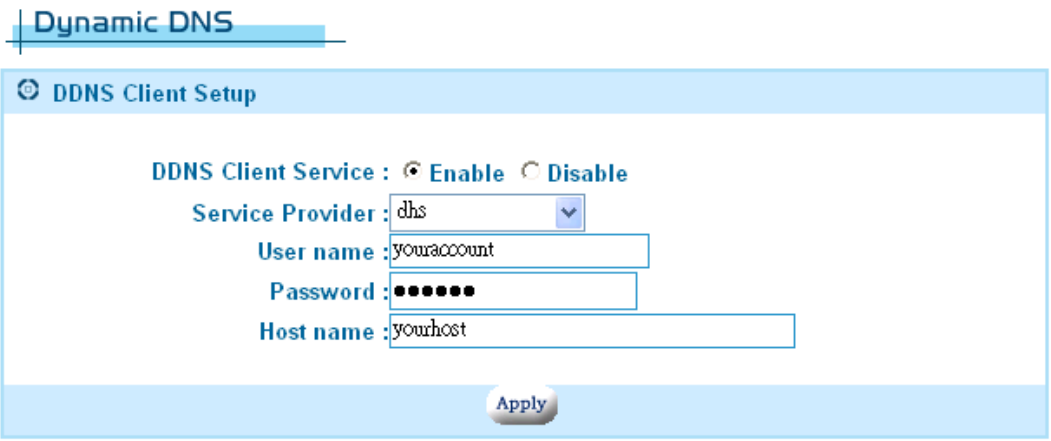
1. Select **Enable** radio button in **Routing Setup**.
2. Enter the network in Destination network column. (e.g. “192.168.6.0/24”)
3. Enter IP address of the gateway in Gateway column. (e.g.

"172.16.1.249")

4. Enter the number in Hop count column. The number means how many gateways you have to pass through.
5. Click the apply button.

In the figures, the destination network is "192.168.6.x". And the packets will be route in or out of the destination network through the gateway "172.16.1.249".

DDNS



Your Internet Service Provider (ISP) provides you at least one IP address to use when connecting to the Internet. The address you as assigned may be static, meaning it never changes, or more than likely dynamic, meaning it's likely to change periodically. How often it changes depends on your ISP. A dynamic IP address complicates remote access since you may not know your current WAN IP address when you want to access your network over the Internet. DDNS provides a simple, and in most cases free, solution.

The Internet uses DNS servers to lookup domain names and translates then into IP addresses. Domain names, such as www.yahoo.com, are just easy to remember aliases for IP addresses. A dynamic DNS service provides a means of updating your IP address so that you listing will be current when your IP address changes. There are several services on the Internet that are available for free. We will only cover one, www.dyndns.org. You will need to register with the service and setup a

domain of your choice from the list they provide for you.

The DDNS service in our device works by uploading your new WAN IP address to the servers when it changes. You would only need to enter the account information in the DDNS setup page of your unit.

How to setup a DynDNS DDNS account:

1. Access the DynDNS homepage (www.dyndns.org).
2. If you have not registered, click ‘Sign Up Now’ to create a new account.
3. Follow the instructions to create a free DDNS account. Requires only e-mail address.
4. Log into your account by providing a username and password.
5. Select ‘Services’ from the top menu.
6. Select ‘Dynamic DNS’ from the choice of services.
7. Select ‘Add A Host’ from the ‘Your Hosts’ section. Follow the instructions.
8. Note your hostname so you can input it in the DDNS configuration for your device.

You can setup additional host names for additional devices.

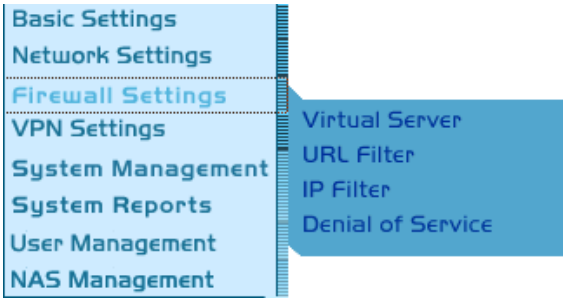
Please follow the steps below to setup DDNS on your SA.

1. Select Enable radio button in DDNS Client Service field.
2. Select the DDNS service provider.
3. Enter the User name. The user name you log in DDNS service.
4. Enter the password. The password you log in DDNS service.
5. Enter the Host name. The host name you register in DDNS service.
6. Click the apply button.

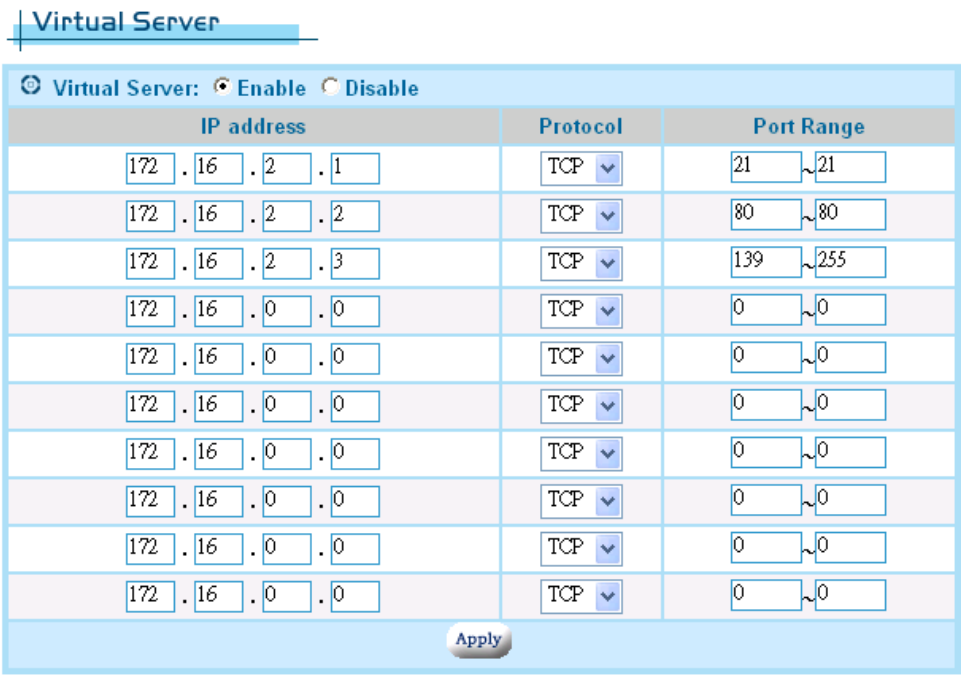
Every time your public IP changes, theAIRIS Power Serverwill tell the DDNS server what your new IP address is. Other users, through the magic of DDNS, will be sent to the right place.

Firewall Settings

When you select the Firewall Settings item in left menu of the web page, four configuration items appear including: Virtual Server settings, URL Filter, IP Filter setup and Denial of Service. Please refer the corresponding section for each of these items.



Virtual Server Settings


Virtual Server
Virtual Server: Enable Disable
IP address
Protocol
Port Range
172 . 16 . 2 . 1 TCP 21 ~ 21
172 . 16 . 2 . 2 TCP 80 ~ 80
172 . 16 . 2 . 3 TCP 139 ~ 255
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
172 . 16 . 0 . 0 TCP 0 ~ 0
Apply

The virtual server service is a way to simulate multiple servers on the intranet. You have several IP addresses within your LAN. These IPs are not visible to the users from the Internet. When servers are installed in the office that need to be seen from the Internet, we establish some

forwarding rules to deal with the packet from the Internet users and direct theAIRIS Power Serverto forward the specific packets to the specific IP address. Users from the Internet could be allowed to access the specific server on your LAN. You can configure different IPs to act as different virtual servers. For example, the users accessing port 21 will be directed to “172.16.2.1”. “172.16.2.1” could be a FTP server. Users accessing port 80 will be directed to “172.16.2.2”, an HTTP server on the LAN. For users outside the LAN, they will feel like many services are running on a single host. Please follow the steps below.

1. Select Enable radio button in Virtual Server.
2. Enter the **IP address** , in LAN will be set as a virtual server.
3. Select the Protocol.
4. Enter the **number** in Ports, the users accessing the port will be directed to the virtual server in step 2.
5. Please repeat the steps above to establish more virtual servers or enter “0” in each field for none.
6. Click the apply button.

URL Filter Setup

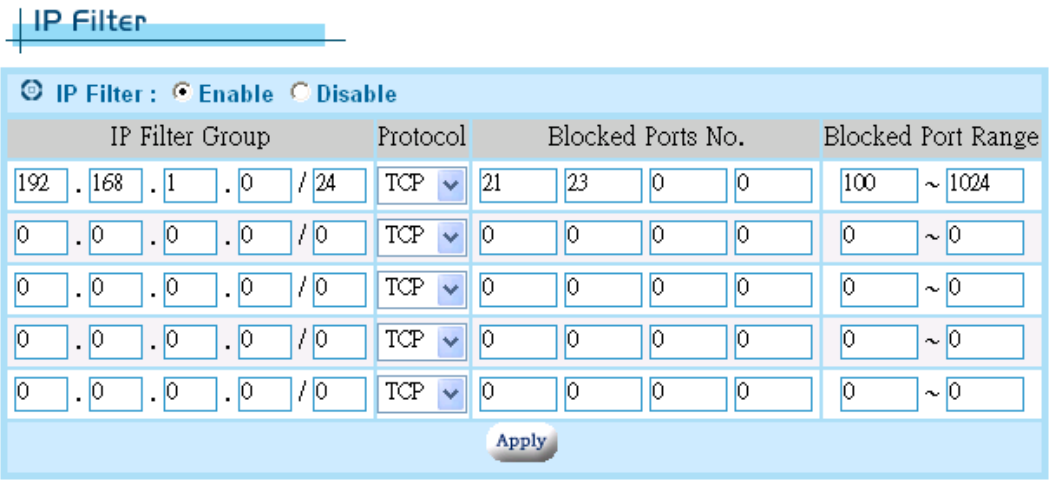
The URL Filter function is used to restrict internal hosts from accessing specific URL locations. You deny any access to the URL location specified in the **Site1**, **Site2** …**Site10** fields.

Please follow the steps:

1. Select Enable radio button in URL Filter.
2. In Site 1, please enter the URL address.
3. Please repeat the step 2 to build more URL addresses not allowed.
4. Click the apply button.

If the **Site1** is given as www.yahoo.com, any hosts in the intranet will not be allowed to connect to www.yahoo.com. If you do not restrict any access from intranet to Internet, please select the **Disable** radio button in the URL Filter.

IP Filter Setup



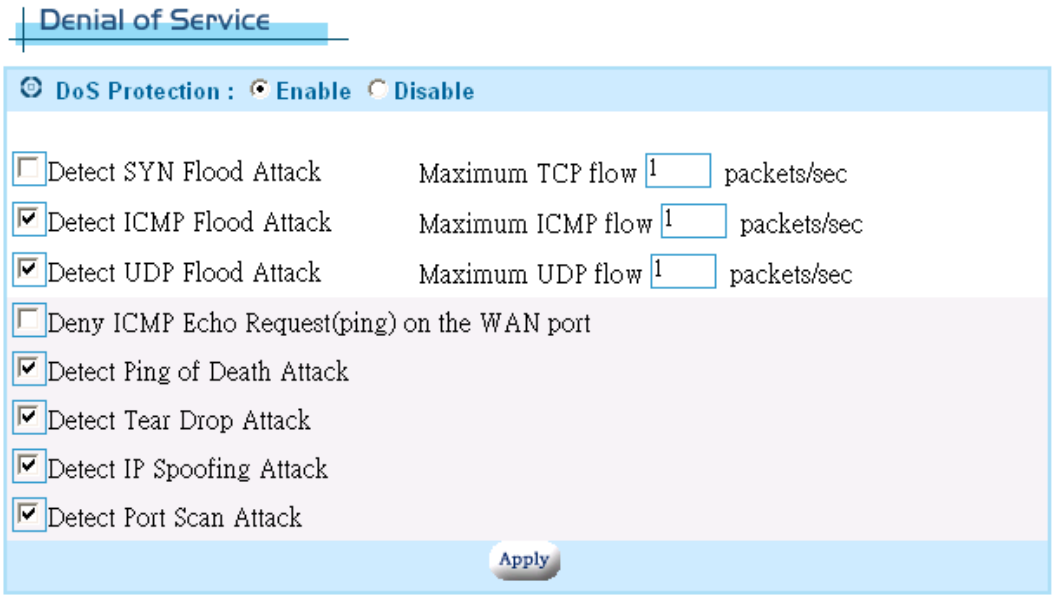
The IP filter function is similar to URL Filter. It provides further restrictions in access permission. URL Filtering only blocks port number 80 (HTTP). In IP filtering, you can assign a group of IP to be restricted. You can block four individual ports or a range of ports in the same time. So the specific group of intranet hosts cannot connect to these ports. Please follow the steps:

1. Select Enable radio button in IP Filter.
2. Enter the IP address range in the format “x. x. x. x / x”(e.g. “192.168.1.0/24”, you would like to restrict the IP group)
3. Select the Protocol.
4. Enter the port number in **Blocked Ports No.** There are four fields you can enter in any order or combination. You can enter one, two, etc.

5. Enter the range of port numbers (if any) in **Blocked Port Range**.

In the example, if any hosts that requests information from 192.168.1.1 to 192.168.1.254 in the intranet with port number 21, 23 or from 100 to 1024 with TCP protocol, will be blocked.

Denial of Service


Denial of Service
DoS Protection : Enable Disable
Detect SYN Flood Attack
Maximum TCP flow 1 packets/sec
Detect ICMP Flood Attack
Maximum ICMP flow 1 packets/sec
Detect UDP Flood Attack
Maximum UDP flow 1 packets/sec
Deny ICMP Echo Request(ping) on the WAN port
Detect Ping of Death Attack
Detect Tear Drop Attack
Detect IP Spoofing Attack
Detect Port Scan Attack
Apply

It is highly recommended that the DoS Protection feature be enabled to prevent attacks on the network. However, if you allow someone to manage the router from outside or are running a web server, e-mail server, or FTP server, you should either disable **Detect SYN Flood Attack** or increase the TCP flow. Otherwise, the configuration web pages will not be sent smoothly.

VPN Settings

VPNs (Virtual Private Networking) provide secure communication between two separate networks without using a dedicated leased line. In order to achieve this functionality, a secure tunnel must be built between the two sites for secure communication over the Internet. TheAIRIS Power Serversupports the most popular protocol - PPTP. PPTP (Point-to-Point Tunneling Protocol), described in RFC 2637 is a PPP-specific protocol proposed by Microsoft. TheAIRIS Power Serverimplements a PPTP server. The remote user can connect to the PPTP server and access a local host behind the PPTP server. When you select the VPN item in left menu of the web page, PPTP configuration options will appear. Please refer to the corresponding section for these configurations.

PPTP Settings

For most companies, the PPTP server creates a secure connection that a remote user can access a host within the company. The remote user has to run a PPTP client and connect to the PPTP server. The PPTP server has to validate the remote user as being in the User List in section 9.1. The server certifies the PPTP client with a username and password. After passing the certification, the server will assign a private IP address to the client. The remote user will be treated like a member of the LAN and can access the local hosts inside the company. Please refer to **Appendix A** for more details about configuring a PPTP VPN connection. To run the PPTP server on the company side, please follow the steps below:

1. In PPTP Settings page: Select the Enable button in PPTP Server field. (**Figure 6.1**)
2. Enter the private IP address of the server in Server IP Address field.
3. Enter the Client IP Range. The server will assign the IP to each client within the range.
4. Click the apply button.

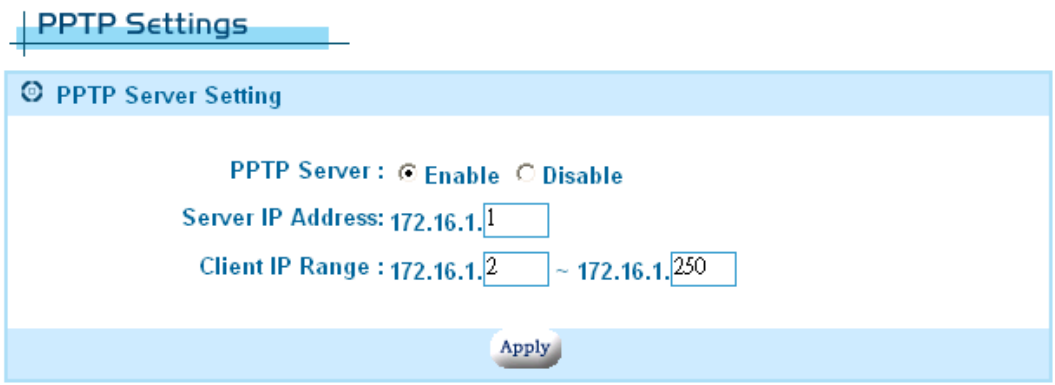
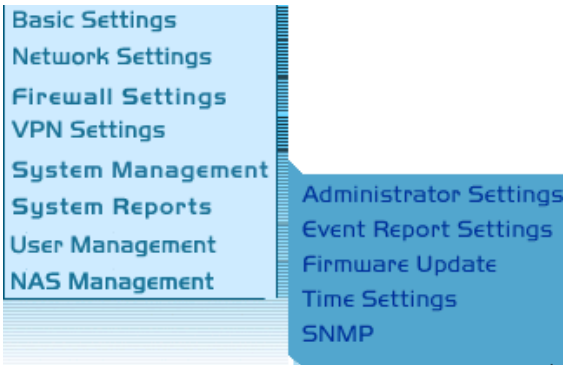

PPTP Settings
PPTP Server Setting
PPTP Server : Enable Disable
Server IP Address: 172.16.1.1
Client IP Range : 172.16.1.2 ~ 172.16.1.250
Apply

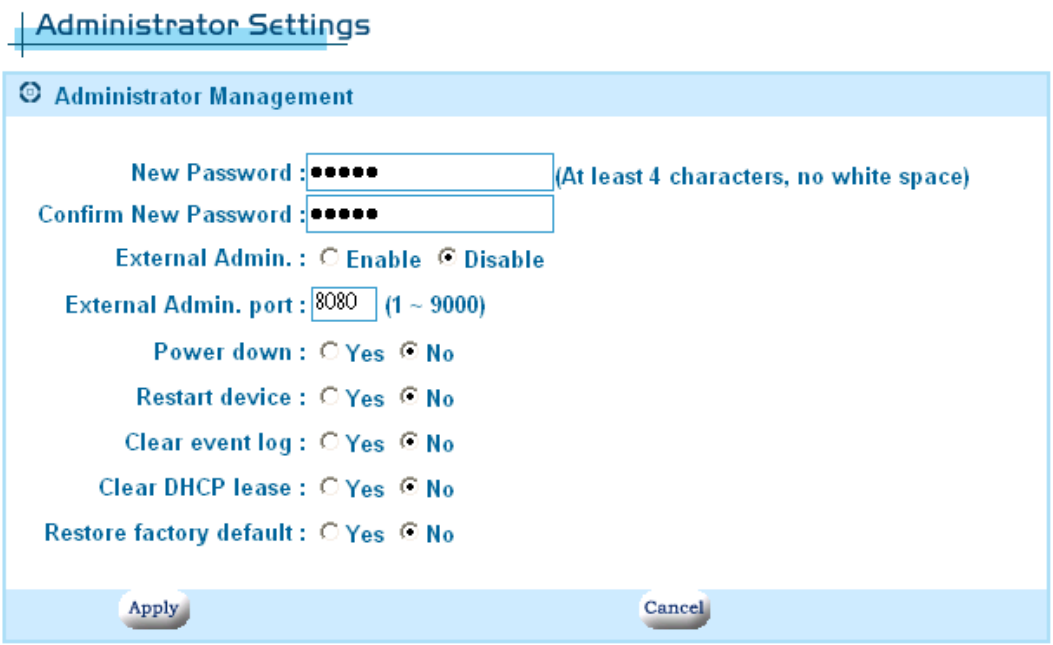
Figure 6.1

System Management

When you select the System Management item in the left menu, four configuration items appear including; Administrator Settings, Event Report Settings, Firmware Update, Time Settings and SNMP. Please refer the corresponding section for these configuration details.



Administrator Settings


Administrator Settings
Administrator Management
New Password :
(At least 4 characters, no white space)
Confirm New Password :
External Admin. : Enable Disable
External Admin. port : 8080 (1 ~ 9000)
Power down : Yes No
Restart device : Yes No
Clear event log : Yes No
Clear DHCP lease : Yes No
Restore factory default : Yes No
Apply
Cancel

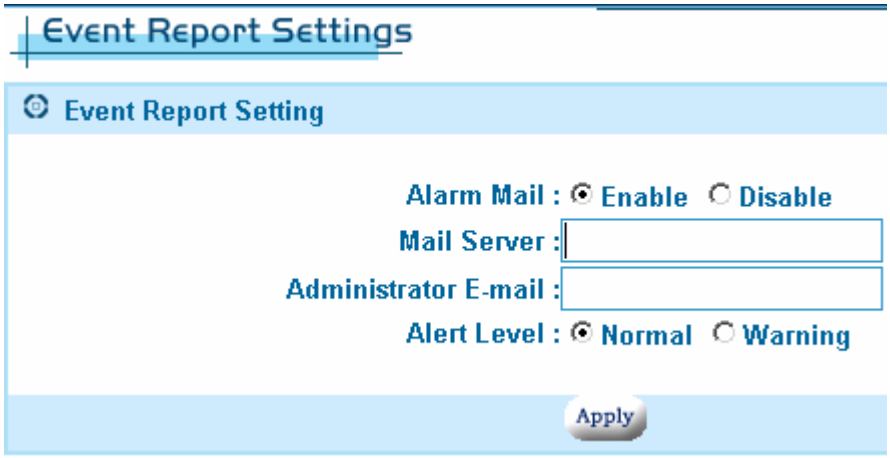
In Administrator settings you will find the basic administrator functions. The settings are easily modified and managed by the administrator. They are described as below:

1. **New Password**: the administrator could change the administrator password here. Please enter the new password you would like to change to. Note that you must fill the new password in both Password change and Password confirmation fields. If both fields are not the same, the page will not be submitted.
2. **FTP Server**: please select the enable radio button to establish the FTP server. Or select the disable radio button for none.
3. **Confirm New Password**: please enter the new password again.
4. **External Admin.**: This feature allows administrators to access the web based configuration menu from the Internet. The default setting for this feature is disabled for security reasons.
5. **External Admin. Port**: defines a port for the remote administrator to connect to.
6. **Restart device**: This function reboots the Powerful Server appliance. Select the enable radio button to restart SA. The default setting of the function is disabled.
7. **Clear event log**: This function is used to clean the system history that is listed in Event Report (section 8.2). If you choose the “No” radio button, the event record never clears even when you reboot the system.
8. **Clear DHCP lease**: This function is used to clean the DHCP Lease record listed in section 8.4. Please choose the “Yes” radio button to clean DHCP lease report.
9. **Restore Factory default**: To recover the factory settings, please choose the “Yes” radio button and the factory defaults will be loaded.
10. **Click the apply button.**

Event Report Settings

Send alerts to an e-mail account. The mail server should allow e-mails from the same network.

E-mail address to send the alerts to.

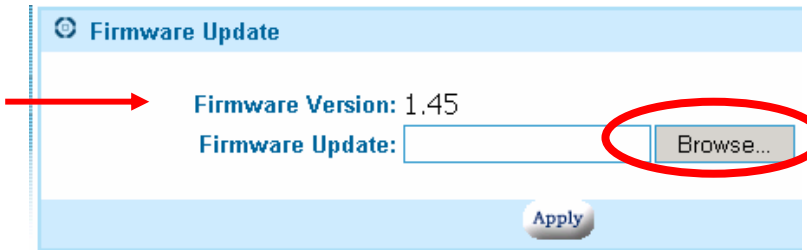


Firmware Update

Updates and functionality can be added via this function. Please check the web for the latest firmware if you are having any issues. In general, no update should be needed unless it is recommended by technical support.

Note: Do not do a firmware update over a wireless connection or power the unit down during a firmware update. Any interruption during an update will damage your unit and require you to send it in for service.

Current firmware version

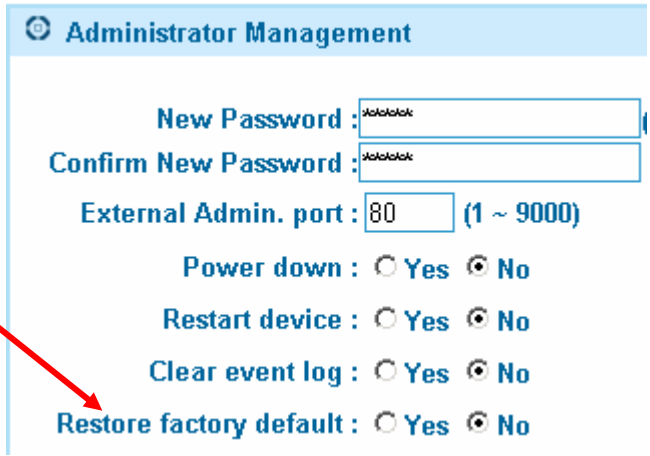


Select **Browse** and locate the updated firmware. If the firmware file is not correct, it will not update the firmware in the unit. The version number will remain the same after the firmware update procedure.

The update percentage will update the status.

Click **Restart** when the upload is complete.

Though it is not generally necessary,

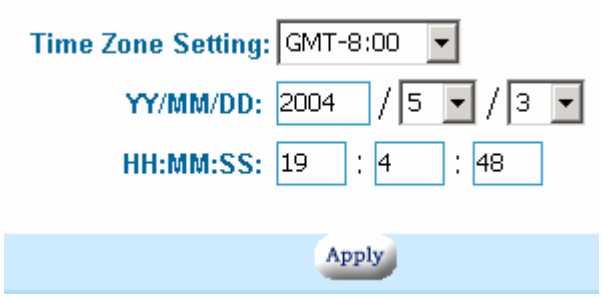

Administrator Management
New Password :
Confirm New Password :
External Admin. port : 80 (1 ~ 9000)
Power down : Yes No
Restart device : Yes No
Clear event log : Yes No
Restart factory default : Yes No

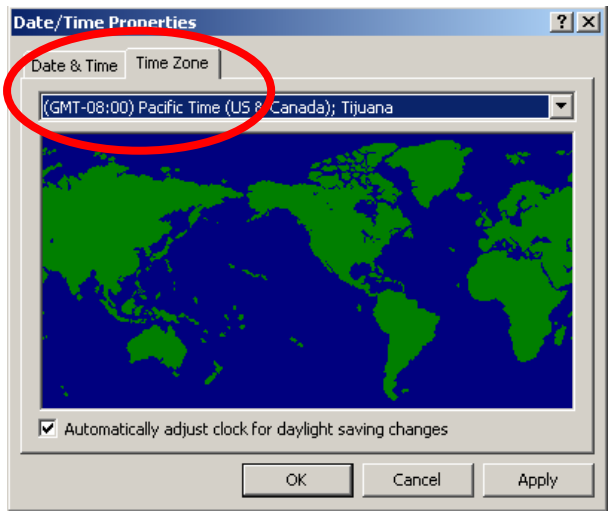
You should restore factory default to make sure that new features and settings are implemented. Note: You must re-initialize the hard drive if you do this.

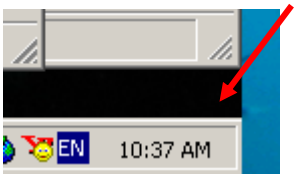
Time Settings

The NAS's built-in clock should be adjusted to the current local time. This will insure accurate time reporting in the logs and file records.

Select your GMT time zone and then enter the date and time. Click on Apply to make the changes.

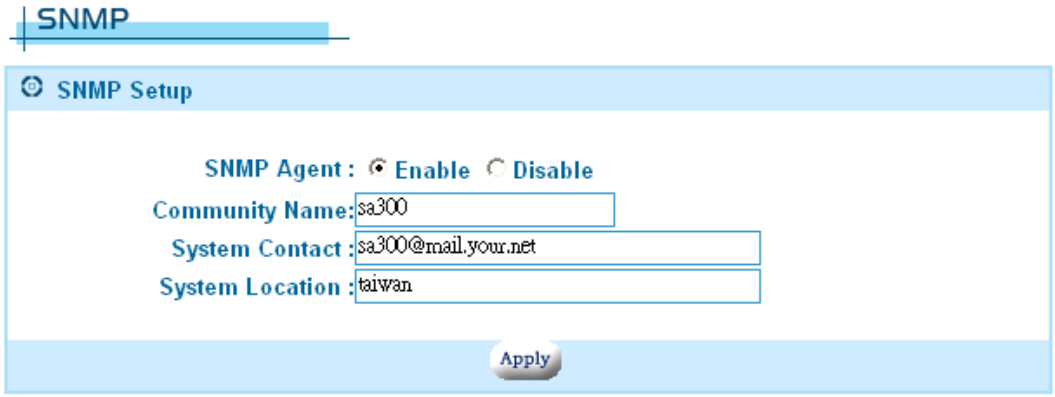






You can find your GMT time zone by double clicking on the clock located on the bottom right corner of your desktop.

SNMP



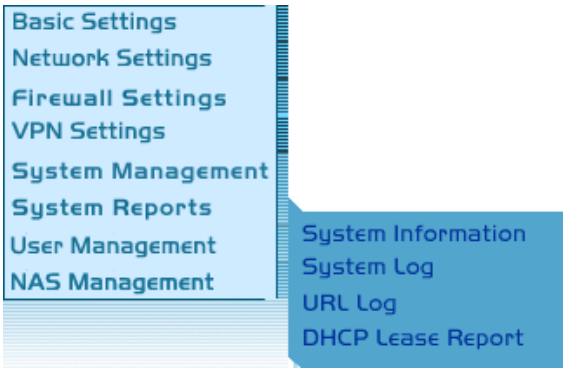
The SNMP agent allows users with SNMP client applications to conveniently inspect the network status of SA.

Please follow the steps below to setup the SNMP agent.

1. Select the Enable radio button in the SNMP Agent field.
2. Enter the Community Name. Note that the agent side and the client side must use the same community name.
3. Enter the contact information in System Contact field. For example, the phone number or the email account of the administrator.
4. Enter the location of the unit the System Location field.
5. Click the apply button.

System Reports

When you select System Reports in the left menu of the web page, four configuration items appear including; System Information, System Log, URL Log, and DHCP Lease Report. Please refer to the corresponding section for these configuration items.



System information

System Report

Firmware Version : 2.02
System Up Time : 0 hour, 36 min, 47 sec

Hard disk Status

Disk Number	Model Name	Size	S.M.A.R.T	Status
HDD-A	ST3300831A	293033 MB	Pass	Ready
HDD-B	ST3300831A	293033 MB	Pass	Ready

Volume Status

Type	Available Size	Total Size	RAID Status
RAID 1(Mirror)	288401 MB	293033 MB	Active , Resyncing

USB Device Information

Position	Vendor	Product ID	Device Type
Port A	--	--	--
Port B	--	--	--
Port C	--	--	--
Port D	--	--	--

External Network Interface

IP Address :192.168.1.106
Hardware Address :00:28:0c:03:2f:0c
Netmask :255.255.255.0
Max. Transfer Unit (MTU) :1500
Tx/Err Packets :340/0
Rx/Err Packets :8266/0
Link Status :Link Up, 100 Mbps, Full Duplex

Internal Network Interface

IP Address :172.16.1.1
Hardware Address :00:e7:4c:35:ef:4c
Netmask :255.255.0.0
Max. Transfer Unit (MTU) :1500
Tx/Err Packets :796/0
Rx/Err Packets :759/0
Link Status (Port 1) :Link Down
Link Status (Port 2) :Link Down
Link Status (Port 3) :Link Down
Link Status (Port 4) :Link Down

Refresh

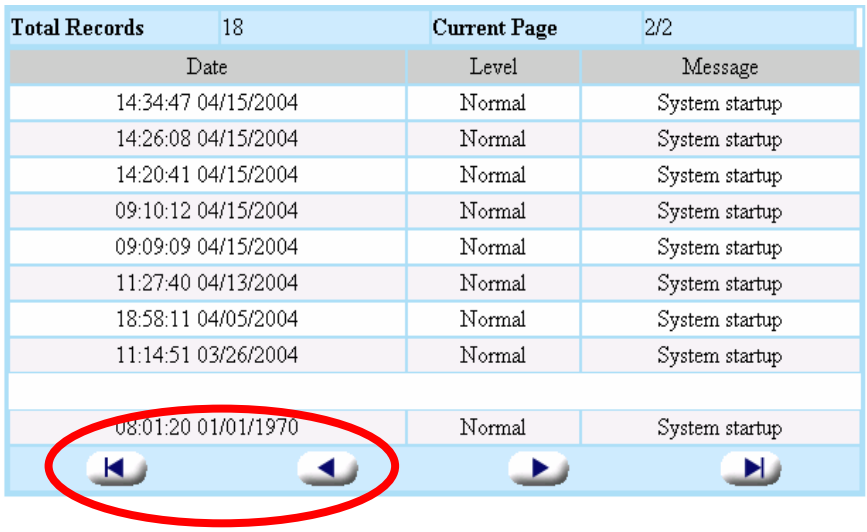
The **System Information** displays some useful information about the system. It shows the firmware version, the system up time and the internal and external network connections. On SA, We have one WAN port and four LAN ports. The WAN port belongs to the external network interface and the LAN port belongs to the internal network interface. They are described as below:

- Firmware Version: 2.00
- The system up time
- IP Address: the IP address is shown as your current setting.
  In Chapter 2, section 2.4, the Basic setting, we already configure the external interface in one of the three ways, ADSL/PPPoE, DHCP client and Fixed IP address. In Chapter4, section 4.1, DHCP Server, we assigned the IP address range to the internal network interface.
- Hardware Address: Ethernet hardware address
- Netmask: corresponding to the network.
- Max. Transfer Unit: maximum bytes of a packet.
- Tx/Err Packets: e.g. 309/0, means you sent 309 packets and there are “0” packets with errors.
- Rx/Err Packets: e.g. 3573/2, it means you received 3573 packets and there are 2 error packets.
- Link Status: Shows the current transfer speed. e.g. 100Mbps, full duplex.
- The refresh button: Click the refresh button to see if anything has been updated.

If your external connection is not set to a fixed IP address, you can check whether the Powerful Server appliance has obtained an IP address after booting. If there is no external IP address, you should check your network connection or environment settings.

System Log

Use the information provided here to help diagnose any network related issues.

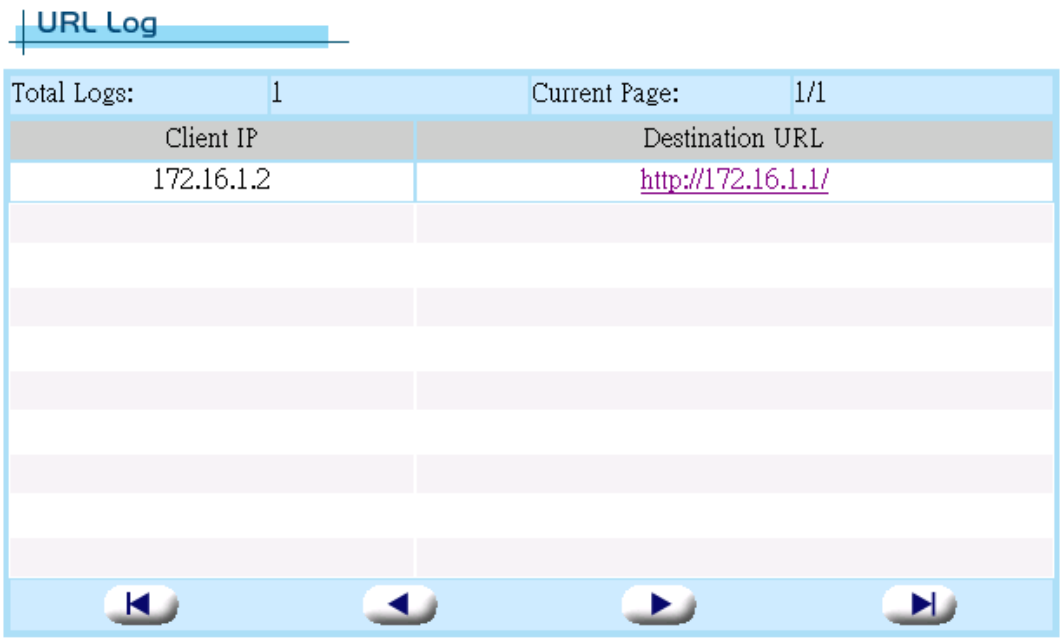


Total Records	18	Current Page	2/2
Date		Level	Message
14:34:47 04/15/2004		Normal	System startup
14:26:08 04/15/2004		Normal	System startup
14:20:41 04/15/2004		Normal	System startup
09:10:12 04/15/2004		Normal	System startup
09:09:09 04/15/2004		Normal	System startup
11:27:40 04/13/2004		Normal	System startup
18:58:11 04/05/2004		Normal	System startup
11:14:51 03/26/2004		Normal	System startup
08:01:20 01/01/1970		Normal	System startup

Navigate through the history with these buttons.

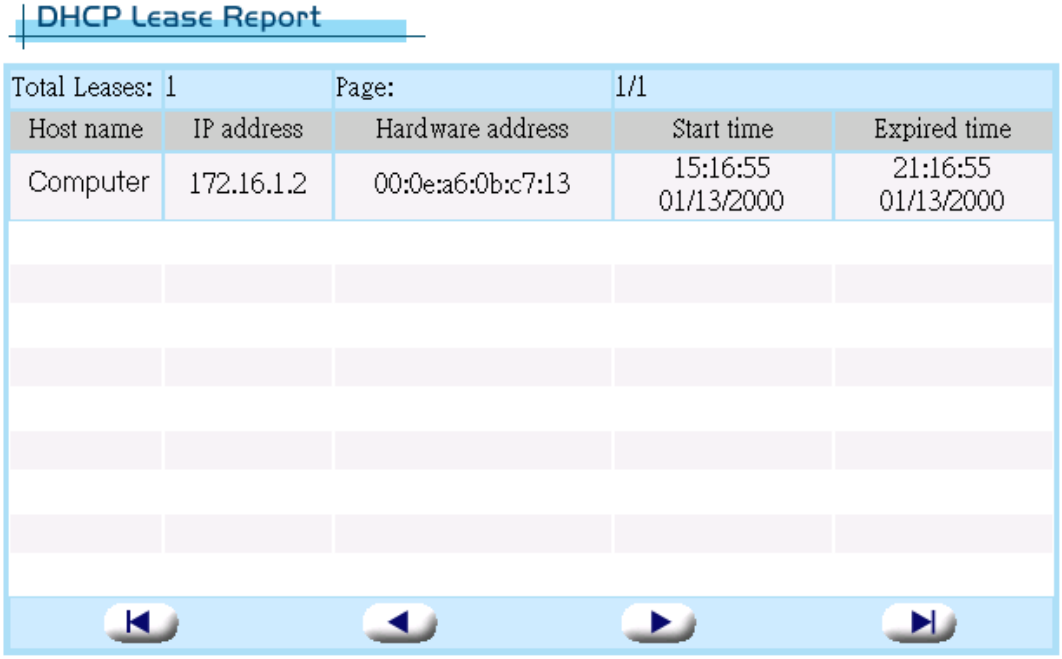
You can clear the event logs under the **Administrator settings** page.

URL Log



The **URL Log** function records the recent connections for each client. If you would like to view what the user is browsing, you can click the corresponding **Destination URL** in the rightmost column.

DHCP Lease Report



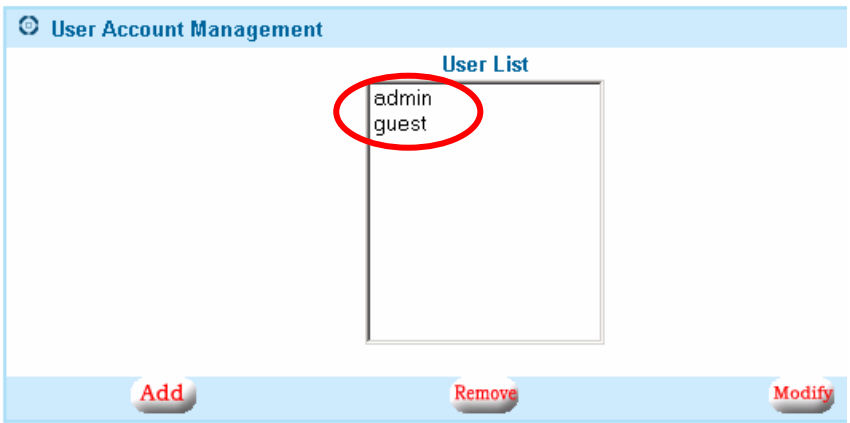
The **DHCP Lease Report** function reports all leased IP provided by DHCP server. From this page, you can find out which host was assigned to which IP address. You can clear all the records through administrator settings. Please refer to the section 7.1, Clear DHCP Lease.

User Management

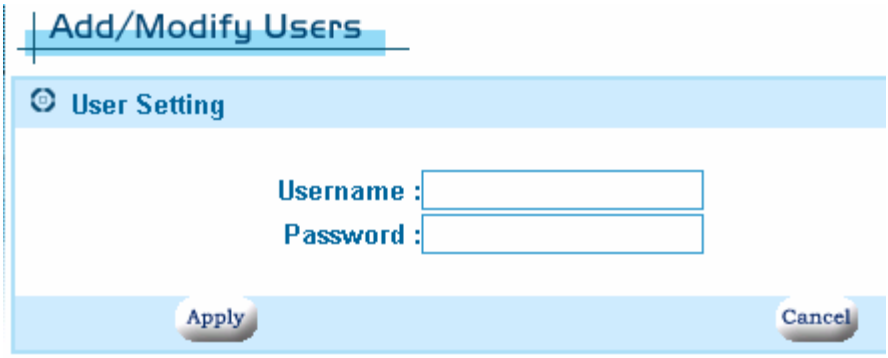
The NAS provides a client/server environment for users to share files over the network. File sharing works by authorizing the users or groups to access shared folders by their username and password. When creating a new shared folder, user and groups from the current list must be assigned. When a user/group tries to access the folder, the system will check the list of valid users for the shared folder. If the user/group is included in the list, the user/group then has permission to access the shared folder.

Users

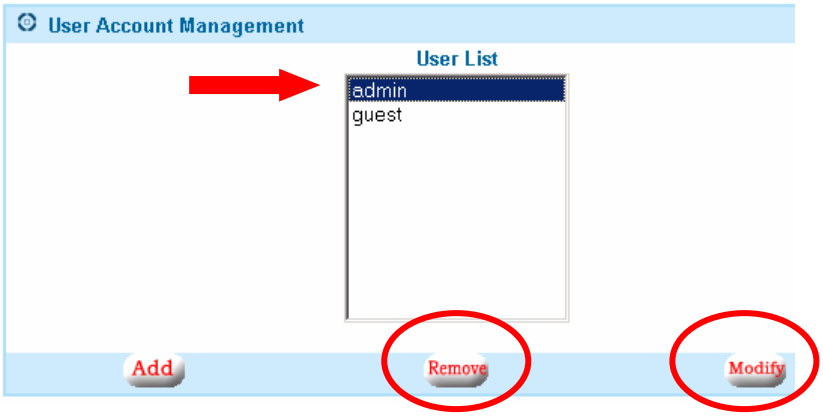
For file sharing to work, we have to allow users and/or groups. We create the user accounts here. The **admin** and **guest** accounts are in the system by default and cannot be removed. The **admin** account is different than the one used to access the UI and can be modified.



Enter a username and password. **Note:** Windows 98 SE, Me users should user the same username as their Windows login. Passwords are recommended, but are not required. Click **Apply** when completed.



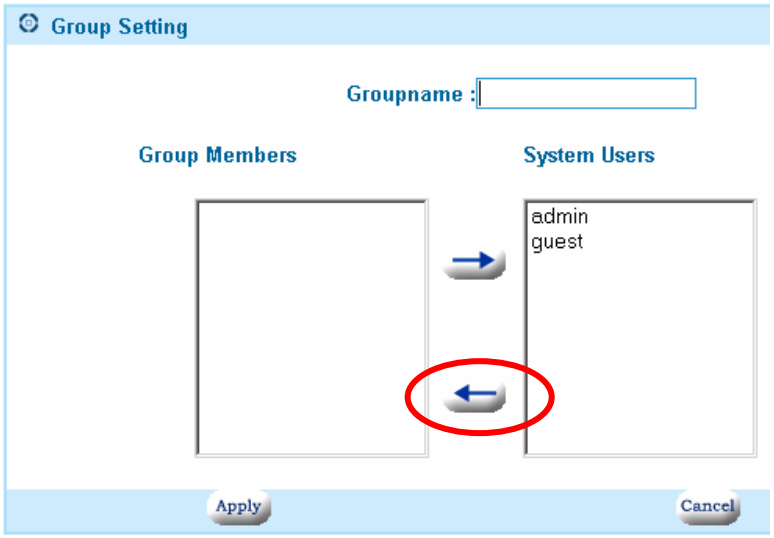
Highlight a user name and click on **Remove** or **Modify** to delete or change user information.



Groups

After creating the users, you can categorize the users into different groups to make assignment easier.

Click on **Add** to create a new group name.

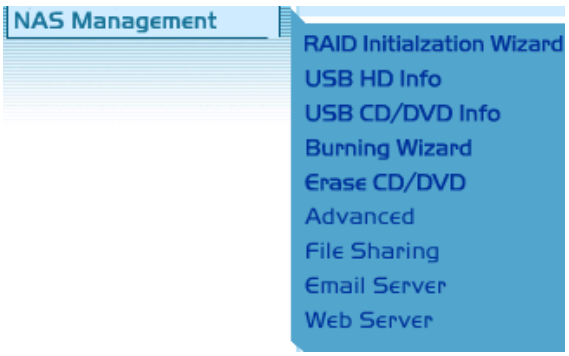


Enter the group name

Highlight the user(s) on the right side and click on the ← button to assign the user(s) to the group. Highlight multiple users by holding down the **Shift** key or **Ctrl** key while selecting users. Select users on the left side and click on the → button to remove them from the group. When complete, click the **Apply** button.

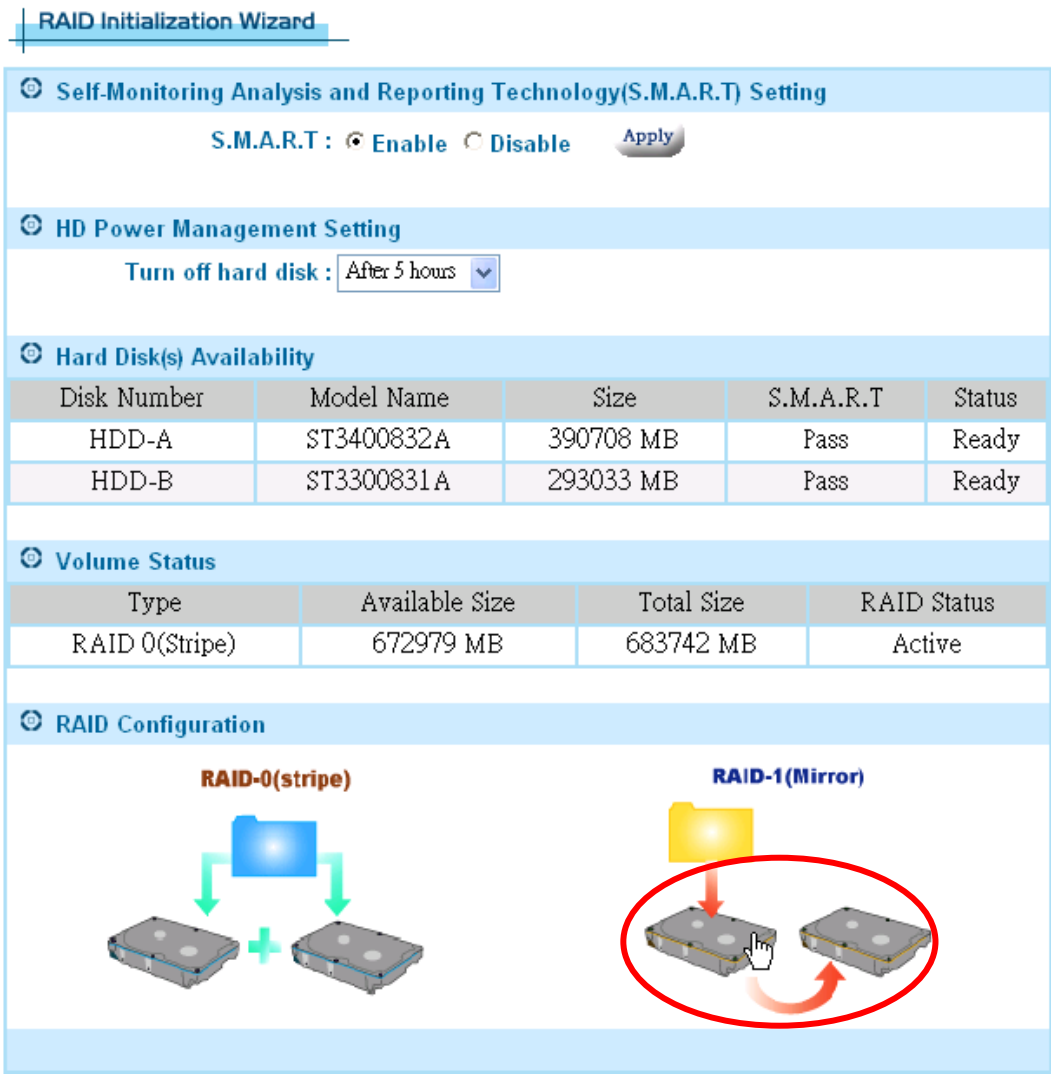
NAS Management

Manage the main functions of the shared storage from this menu.



RAID Initialization Wizard

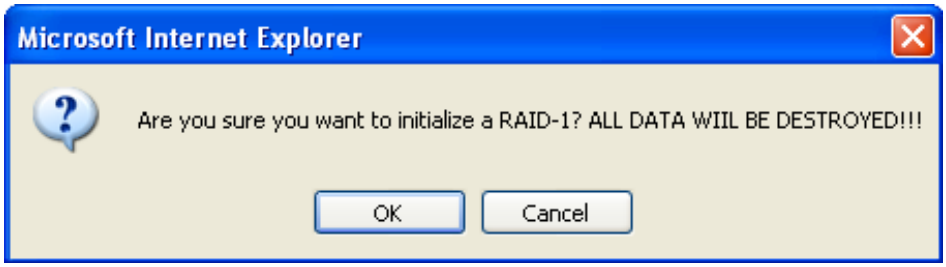
The first time you use the NAS, you may have to initialize the hard disk. The wizard provides an easy way to initialize the hard disk.


RAID Initialization Wizard
Self-Monitoring Analysis and Reporting Technology(S.M.A.R.T) Setting
S.M.A.R.T : Enable Disable Apply
HD Power Management Setting
Turn off hard disk : After 5 hours
Hard Disk(s) Availability
Disk Number | Model Name | Size | S.M.A.R.T | Status
HDD-A | ST3400832A | 390708 MB | Pass | Ready
HDD-B | ST3300831A | 293033 MB | Pass | Ready
Volume Status
Type | Available Size | Total Size | RAID Status
RAID 0(Stripe) | 672979 MB | 683742 MB | Active
RAID Configuration
RAID-0(stripe)
RAID-1(Mirror)

By enabling SMART, the NAS will report when the hard drive is about to fail. Your hard drive must support this feature.

The HD Power Management should be enabled to prolong the life of the hard drive. When there is no activity for the set time period, the hard drive will power down to conserve power, save wear and tear, and prevent the unit from building up unnecessary heat. When a user wants to access the storage, the NAS will automatically wake up.

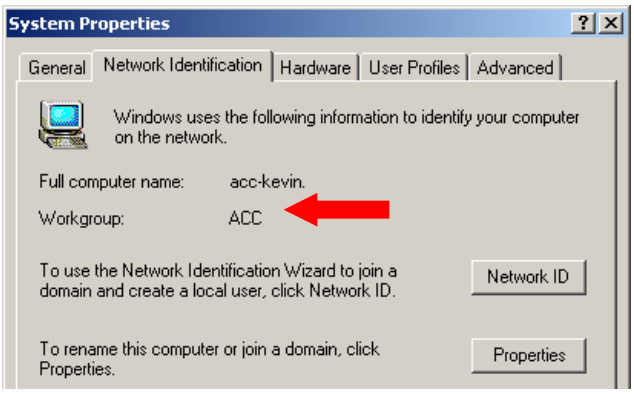
Select the type of RAID you want to apply above then click on the icon to begin the initialization process.



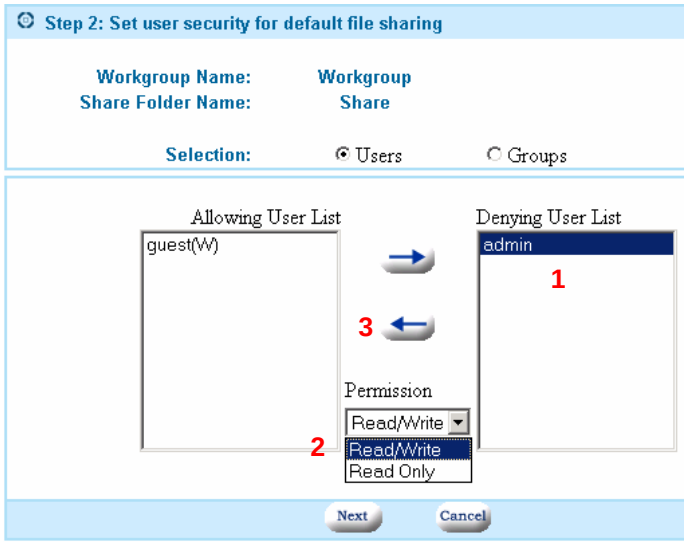
Click **OK** to the warning message to continue the process.

Enter the workgroup name, description and initial share folder name. The workgroup name should be the same one that the computers accessing the NAS are on. Windows 2000/XP users can use a different workgroup name if desired. Click **Next** to continue.

You can find your workgroup name by right clicking on **My Computer** and selecting **Properties**.


System Properties
General
Network Identification
Hardware
User Profiles
Advanced
Windows uses the following information to identify your computer on the network.
Full computer name: acc-kevin.
Workgroup: ACC
To use the Network Identification Wizard to join a domain and create a local user, click Network ID.
Network ID
To rename this computer or join a domain, click Properties.
Properties

You must assign at least one user to this share folder. (**1**) Highlight the user on the list to the right, (**2**) select the permission you want them to have: Read/Write or Read Only, (**3**) click on the ← button to move the user over to the Allowing User List.



Highlight users on the left list and select the → button to remove them from the share or change their permissions.

Click **Next** to continue.

The progress of the initialization will be displayed.

You can also view the progress by returning to the main wizard screen.

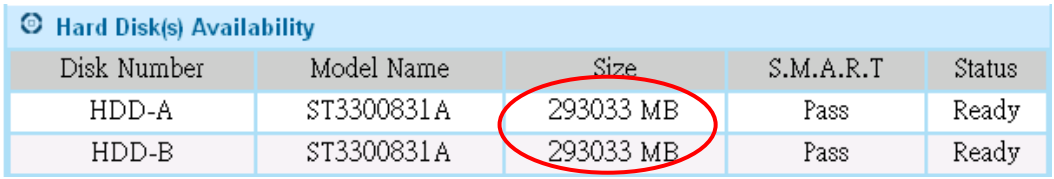
S.M.A.R.T	Status
Disable	Formating(18%)

Once the HDD is formatted, the status will change to **Ready**. If you select RAID 1, you will also see progress of resyncing on RAID Status field.

Total Size	RAID Status
293033 MB	Active ,Resyncing(1%)

S.M.A.R.T	Status
Disable	Ready

Disk size will be shown in size field column as illustrated in Figure 3.8a

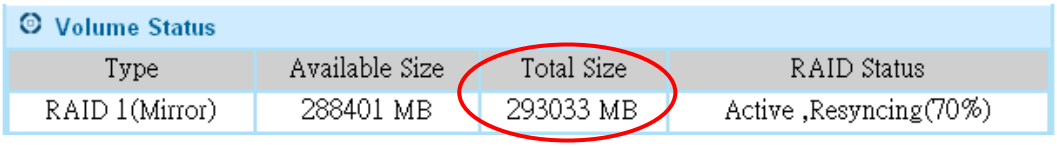


Hard Disk(s) Availability

Disk Number	Model Name	Size	S.M.A.R.T	Status
HDD-A	ST3300831A	293033 MB	Pass	Ready
HDD-B	ST3300831A	293033 MB	Pass	Ready

Figure 3.8a

After initializing to RAID 1 (Mirror), you should see a screen similar to Figure 3.8b where total size is the same as the original hard disk size. If the size of



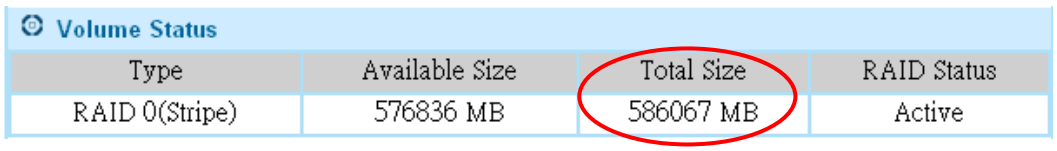
Volume Status

Type	Available Size	Total Size	RAID Status
RAID 1(Mirror)	288401 MB	293033 MB	Active ,Resyncing(70%)

Disk 1 and Disk 2 is different, then RAID 1's total size would automatically select the smaller one as its baseline. However, we suggest you to use the same size when choosing RAID 1.

Figure 3.8b

After initializing to RAID 0 (Stripe), as shown in Figure 3.8c, you can see that total size is the sum of two hard disks. Please be reminded that the total size of RAID 0 would always be the sum of Disk 1 and Disk 2.



Volume Status

Type	Available Size	Total Size	RAID Status
RAID 0(Stripe)	576836 MB	586067 MB	Active

Figure 3.8c

In System Information page, when Powerful Server cannot detect hard drive (Status of Disk 1 as illustrated in Figure 3.8d) or detect an error in S.M.A.R.T. (Status of Disk 2 also illustrated in Figure 3.8d), you will see "Not Active"

shown in status field.

Hard Disk(s) Availability

Disk Number	Model Name	Size	S.M.A.R.T	Status
HDD-A	--	--	--	Not Actived
HDD-B	QUANTUM FIREBALL ST2.1A	2062 MB	Failed	Not Actived

Figure 3.8d

When Powerful Server detect hard drive in “Not Active” mode, RAID will not be activated (Figure 3.8e).

Volume Status

Type	Available Size	Total Size	RAID Status
No Available			

Figure 3.8e

As long as there’s a hard disk either in “Not Active” mode or in initialization process, user would be able to execute RAID initialization. You will see a screen similar to Figure 3.8f shown on your screen where the button would be disabled in grayish color.

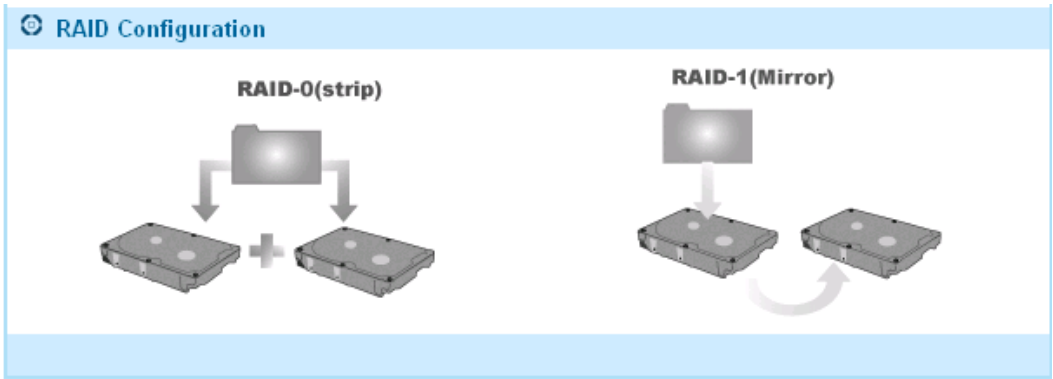
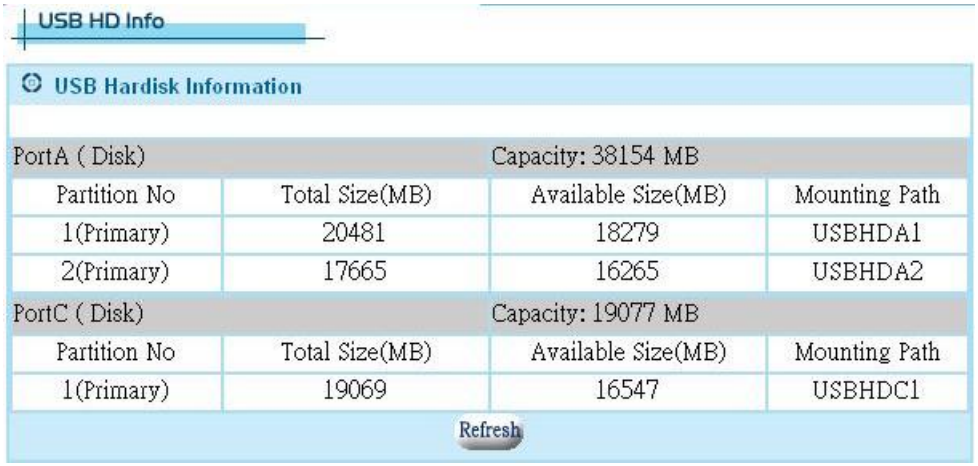


Figure 3.8f

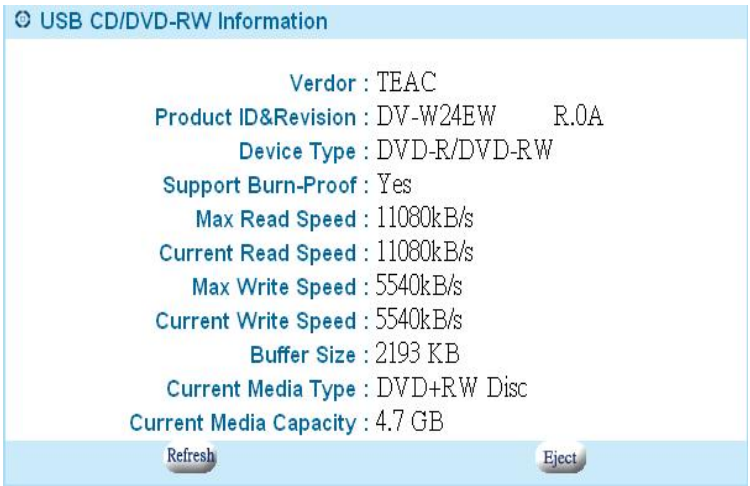
USB HD Information

Each of formatted partitions (FAT32, EXT2 and EXT3) on the attached USB storage drive will be shown in the USB HD information page. The naming rule for “Mounting path” is based on the connecting port. For example, if the USB hard drive was attached on port A and here are three formatted primary partitions on the disk, theAIRIS Power Serverwill create "USBHDA1" and "USBHDA2" mounting path to represent each partition space.



USB CD/DVD-RW information

This page display more detailed information for the connected USB CD/DVD-RW device. The device type, transfer speed, media type and media capacity will be shown in this page. The “Refresh” button let you can update the Information immediately and “Eject” button is used to unload the current media (open the tray).


USB CD/DVD-RW Information
Verdor : TEAC
Product ID&Revision : DV-W24EW R.0A
Device Type : DVD-R/DVD-RW
Support Burn-Proof : Yes
Max Read Speed : 11080kB/s
Current Read Speed : 11080kB/s
Max Write Speed : 5540kB/s
Current Write Speed : 5540kB/s
Buffer Size : 2193 KB
Current Media Type : DVD+RW Disc
Current Media Capacity : 4.7 GB
Refresh
Eject

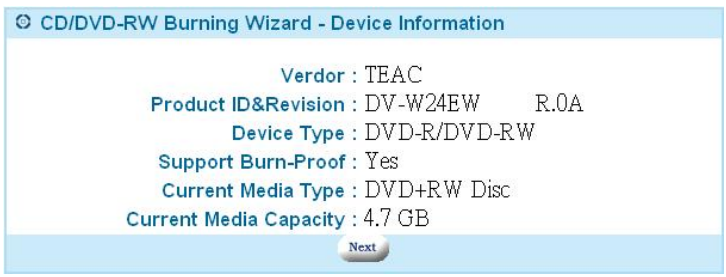
Erase CD/DVD

Before you erase CD/DVD-RW disc, the current media information will be shown as the picture on the right side. The most important thing is you can know how much data have been stored in this disc. When you press the “Apply” button on the “Current Media Information” page, the warning dialog will be pop-up , it will remind you all data will be destroyed after erasing the disc.

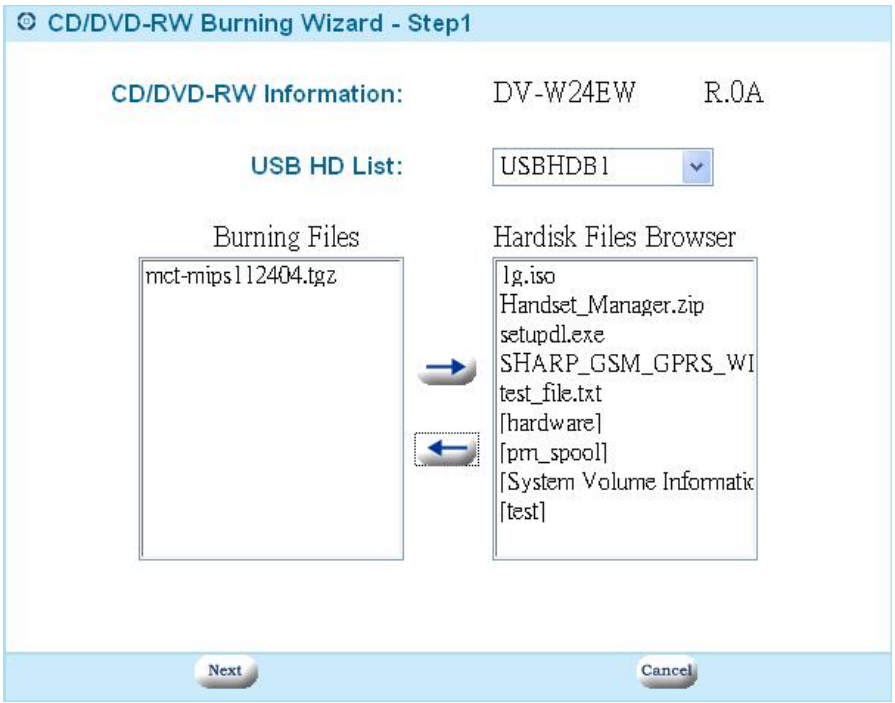
Current Media Information
Verdor : TEAC
Product ID&Revision : DV-W24EW R.0A
Device Type : DVD-R/DVD-RW
Current Media Type : DVD+RW Disc
Data Size on Disc : 109 MB
Apply

Burning Wizard

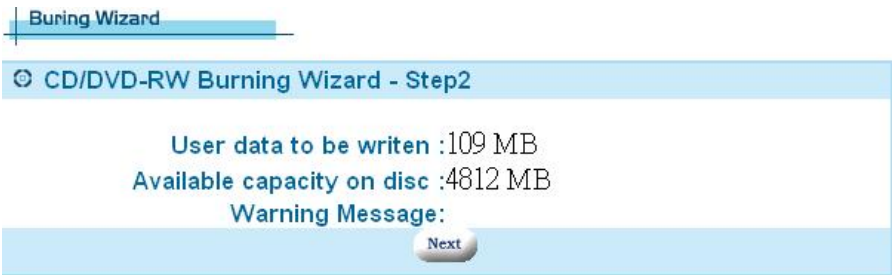
The convenient burning tool be provided here, you don’t need to backup your USB data into CD/DVD-RW disc through the windows application, just follow the instructions of the burning wizard, you can easy to backup your important files into connected USB CD/DVD-RW. The “Device Information” will be shown first. Before burning, you can check all information here.


CD/DVD-RW Burning Wizard - Device Information
Verdor : TEAC
Product ID&Revision : DV-W24EW R.0A
Device Type : DVD-R/DVD-RW
Support Burn-Proof : Yes
Current Media Type : DVD+RW Disc
Current Media Capacity : 4.7 GB
Next

Next, you can select files to backup from the connected USB HD in the Step1 page. All available USB storage be shown in the USB HD List. Highlight the file(s) on the right side and click on the ← button to select the burning file. Select the files on the left side and click the → button to remove file from burning Files list. When complete, press the next to enter next step.



Before starting to write the selected files to the disc, the wizard will show the total amount of your selected files and available capacity on the disc now. If everything is ok, press the next button to start burning.



Please wait the progress bar up to 100% and disc will be ejected automatically when the burning complete.

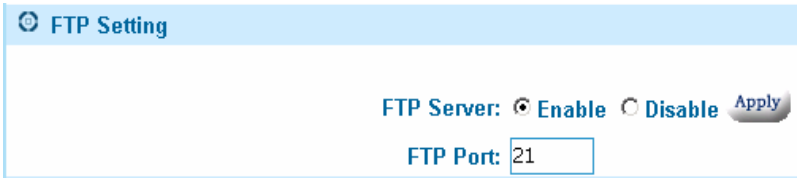
Advanced Settings

All the file protocols settings are located here. Disable any protocols not in use by the computers on the network to increase performance. Most users will not need to change any of the settings. Make sure to click on **Apply** after making any changes.

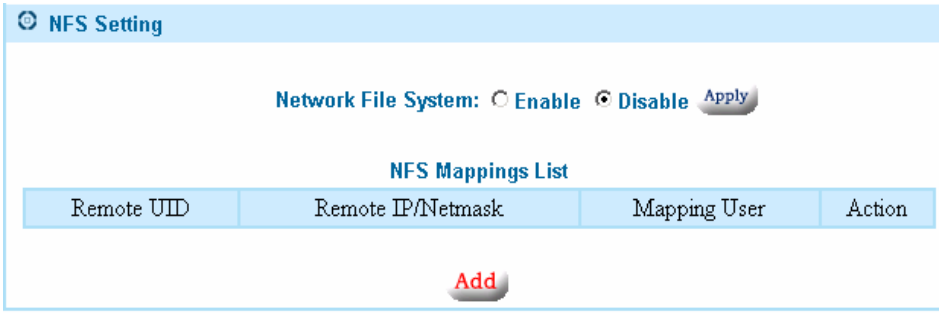
Change the workgroup or NAS description. Workgroup name should be the same for all computers sharing files.

Enable Apple file sharing for compatibility with older Macs.

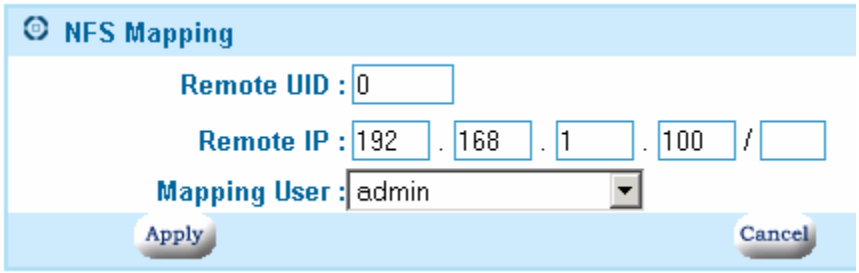
Enable the FTP server to allow remote and local FTP file access. Change the default FTP port 21 for added security or compatibility. **Note:** If you change the default port, users must manually enter the new port number when trying to access the FTP server. See **FTP Server** chapter.



Linux users need to create NFS Mappings in order to connect to the NAS. Enable the Network File System and click on **Add** to create the mapping.



Enter the Remote UID, IP, netmask and the local mapping user.



Once complete, mount the share on the Linux machine. A typical mount command line:

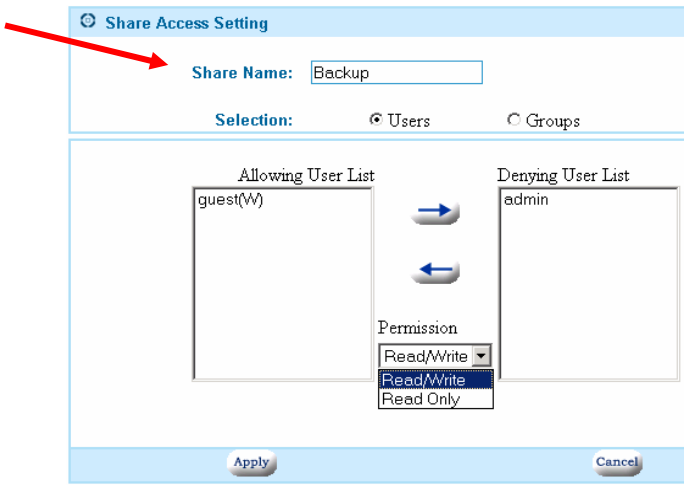
 # mount <IP address>:/<share folder> /<local directory>

File Sharing

For file sharing, you must create users and groups first. Use this to organize the data on the NAS. You can create private and public folders. By managing which users have access to the shares, users can only access information that they are allowed to. This access is the same whether they are accessing the share from the local network or through the Internet via FTP.

Click on **Add** to create a new shared folder.

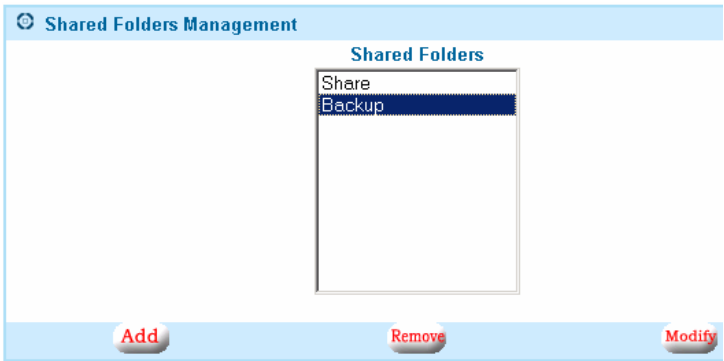
Enter a share folder name



Assign users by highlighting the user, selecting the file permission and clicking on the ← or → button.

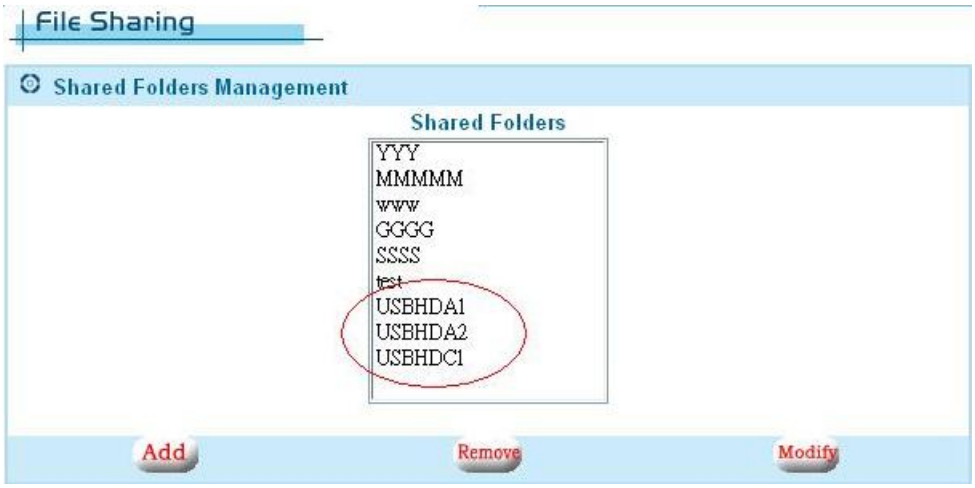
Click on **Apply** when complete.

Highlight the share folder and click on Remove or Modify to delete or edit the shared folder properties.



— For USB Storage Sharing

As mentioned above, each partition of the attached USB storage will be presented to one shared folder. So, if one USB storage device be plugged into A port and it have 2 partitions. The system create the USBHDA1 and USBHDA2 automatically and assigned the guest have read/write permission by default.



FTP Server

If you want to access files stored on your NAS from a remote location, the included FTP server is the easiest way. Here is a typical setup:

Connection Diagram:

Work PC<-->Internet<-->DSL/Modem<-->Router<-->NAS

To access files from the NAS from a remote location, a static IP and/or a DNS name is required. You can also setup a DDNS account if you are using a dynamic IP (your DSL IP changes all the time). See **Dynamic Domain Name Server** for additional information and help in setting up this service. Your router must have this feature or you may have to run client software on a PC that is running on the network. You must set your router to forward **port 21** to

your NAS's **fixed IP address**. Refer to the DDNS and port forwarding/virtual server chapter of your router manual for details.
Enable the FTP server on the NAS.

You can change the default FTP port in the same configuration screen. This is useful for making you FTP server less visible to users whom you do not want to grant access. Some networks also block the standard port 21 and may require you to change to a different port. **Note:** If you change the default port 21, you will need to enter the port number every time you access the FTP server.

Make sure to have users and passwords assigned to all your shared folders. If you want to allow anyone access, just assign the 'guest' account to that folder. FTP users can then log on with and anonymous account to that folder. **Note:** Users will be able see the names of all the other shared folders, but will not be able to access them without a username and password. To completely disable anonymous access (must have user account on NAS to see folders), make sure you do not have the 'guest' account assigned to any shared folder. Now from the remote location, type into a browser (or FTP application) ftp://<DDNS Name> and it will take you to your NAS unit. If you cannot see anything on your browser, make sure you have the 'View FTP Folders' option turned on in your browser settings. You may also have to go into 'File->Login As'. Use a valid user name and password for the NAS.

Personal Web Server

The Web Server settings are currently under 'Nas Management->Web Server'.

Getting started

Enable the web server by selecting the ‘Enable’ radio button. It will then create a shared folder called 'www'. Set the server port number to '80' if you want all default HTTP calls to go to your website. When you type in a URL address in a browser, the Internet automatically directs your browser to port 80 at that address. This is the industry standard and should be used 99% of the time. If you want to hide or make your site available only to people who know your port number, then you can assign it a different port. For example, if you were to assign port 77 instead of 80, users would have to type in their browser www.mywebsite.com:77 to see the website. You do not normally use ‘:80’ because that’s the assumed default in the industry.

Uploading your web page(s)

All web pages for your website will be stored in the ‘www’ shared folder. You can copy the folders and files of your website into that directory via the network neighborhood, mapped drive, or FTP if you have enabled that function. Make sure that you have allowed the user uploading the files to have read/write access under ‘File Sharing’. By default, anyone (anonymous) can have access to the ‘www’ shared folder as the guest account is assigned to that share.

Web page design

You must have an '**index.html**' file as that is what the web server will look for as the first page of your website. You are free to make folders under the ‘www’ directory to help organize your website. All references to those directories can be called on from any page. You can use many popular web page design programs to make your website and then copy the finished product (all associated images, files and folders also) to the ‘www’ shared folder.

Accessing the website

Users with a static WAN IP address can access the website simply by typing in the IP address on any browser. If you are on the inside of the network, you

must use the WAN IP address to access the website, not the internal appliance IP address. If you have a domain name, then you can have the domain name company forward the domain to this static IP address. With a domain name, you do not have to remember the IP address, just the domain name.

If you have a dynamic IP, you can setup a DDNS account and enable the DDNS feature of your appliance to make your website accessible without having to find out the current IP address. Refer to the **DDNS Chapter** for more information.

Important Note:

The ‘www’ share defaults to allow ‘guest’ users to have access. Please go into NAS Management -> File Sharing, add a valid user and remove ‘guest’ if you do not wish everyone to be able to modify you web pages.

E-mail Server

The E-mail Server settings are located under **Nas Management->E-mail Server**.

Getting started

In order to use the e-mail server, you must have a domain name or have registered with a DDNS service provider. E-mail requires a domain name and will not work with just an IP address. Enable the e-mail server by selecting the ‘Enable’ radio button. Enter your domain name in ‘Mail Domain Name’. For example, myhomedomain.com is a valid name. Do not enter the ‘www’ usually associated with domain names. If you have a DDNS name, for example, myname.dyndns.org, you can enter it here in as shown also. You should limit the maximum size a mailbox under the quota field and the size of each e-mail in the following field. Default settings are ‘0’ for unlimited.

E-mail names

After applying the settings, your e-mail accounts are now active. They are based on your user names that are created under user management. For example, if ‘teacher’ is a user on the appliance, and ‘school.com’ is the

domain name, the e-mail address for ‘teacher’ is now ‘teacher@school.com’. DDNS e-mail addresses work in a similar manner. For example, if ‘teacher’ is the user on the appliance and the domain name (DDNS) is ‘school.dyndns.org’, then the e-mail address would then be ‘teacher@school.dyndns.org’.

Sending and receiving e-mail

You can use any POP e-mail type program to retrieve and send your e-mails. Windows includes MS Outlook Express as a standard application. Start Outlook. Under Tools->Mail, you want to ADD a mail account. Enter a display name, the formal name you want your e-mails to appear to come from (Usually your full name). In the e-mail address field, enter your new e-mail address. From the above example, we would enter ‘teacher@school.com’ or ‘teacher@school.dyndns.org’. Under ‘Incoming mail server’ and ‘Outgoing mail server’, enter your domain name. In the above examples, it would either be ‘school.com’ or ‘school.dyndns.org’. Both fields should be the same. Lastly, enter the Account name and password. This name is the same one as on your appliance. In this case, user name is ‘teacher’ and password is: ****. Click on the ‘Finish’ and you are ready to send and receive e-mail!

NOTE:
Passwords are highly suggested for all e-mail account users to protect your e-mails and to prevent people from unauthorized use of your e-mail server.

Windows USB Printer Server

Standard USB 1.1 and 2.0 printers can easily be shared between Windows users on the network with the built-in USB printer server. Note: Some or all functions of multi-function printers may not work depending on the driver support by the respective printer manufacturers.
Please make sure the hard disk has been initialized. (The RAID status is Active)

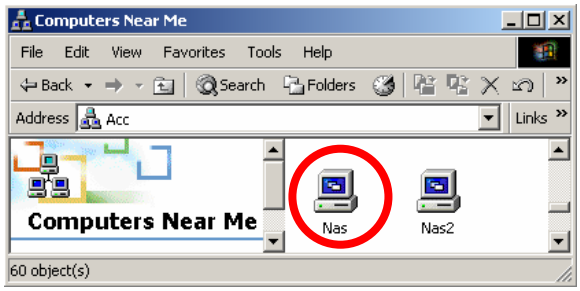
Volume Status

Type	Available Size	Total Size	RAID Status
RAID 0(Stripe)	576836 MB	586067 MB	Active

Connect a USB Printer to the USB port on the back of the NAS and turn it on.

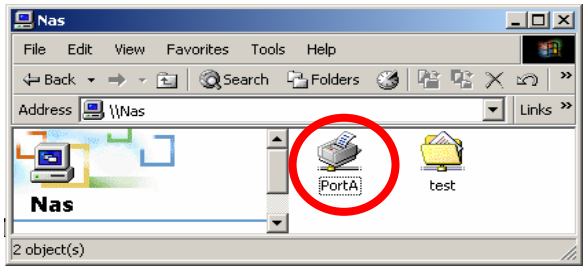
Windows Neighborhood

Locate the NAS device in **My Network Places** and select it by double clicking on the icon.



Enter a valid user name and password when prompted.

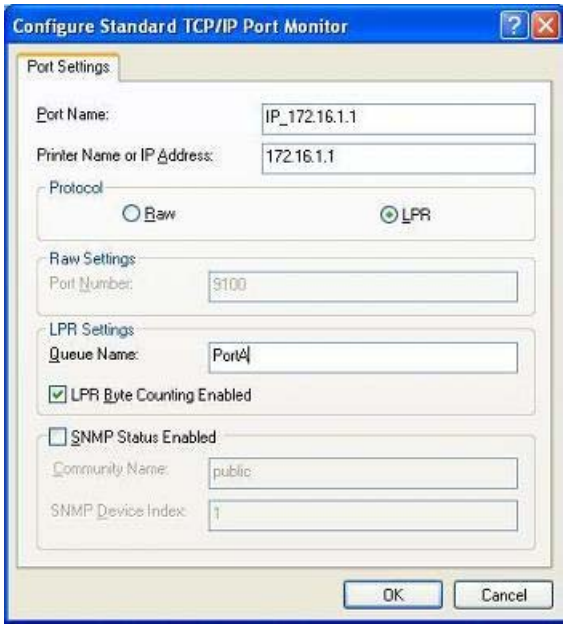
You will now see the printer port next to the shares for the device. Double click on the **PortA** printer icon and follow the instructions to install the printer driver at the local station. You may need to select 'Have Disk' and insert your printer's driver CD during the installation process.

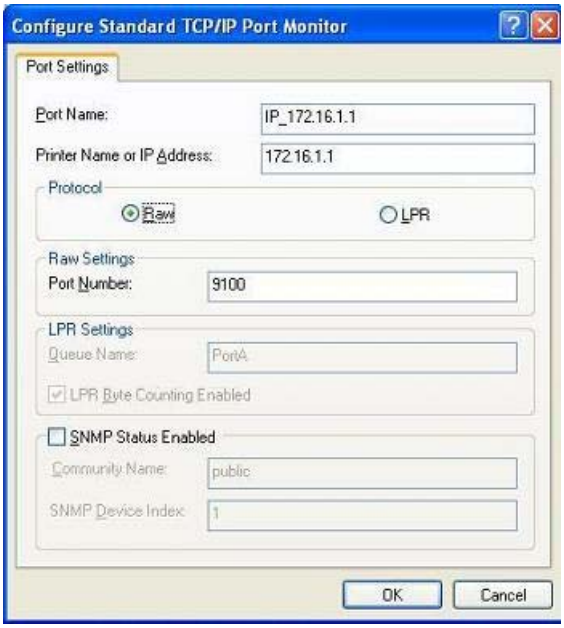


Once the driver installation is completed, you should be able to select the printer from the printer list in any Windows application. You can manage the printer the same way as any other networked printer under Windows.

Standard TCP/IP Port for Windows 2K/XP (LPR & Raw mode)

The following two pictures demonstrate how to setup the TCP/IP printer port under Windows 2K/XP. As mentioned before, if the printer connected to USB port A position, we will name it as “PortA”. So, when you want to setup LPR protocol, the “Queue name” should be filled with which port you plug in. And LPR Byte Counting Enabled is required. For the Raw mode, the port number 9100 is represented as “PortA” and 9101 is PortB , etc.





Appendix A

PPTP VPN (W2K and XP only)

Important:

Make sure that the subnet of your Appliance is different the network you are trying to connect from. For example: User's office IP addresses are 192.168.1.x, set your Appliance to 192.168.2.1 Netmask 255.255.255.0.

Make sure that you have created a user account and password on the Appliance for the users that you want to allow VPN access.

Proceed to your appliance's PPTP Settings under VPN Settings.

1. Enable the Server
2. Enter a server IP, a number from 2-254 that is not being used by any computer on the Appliance network. Usually 200 is a safe number.
3. Enter a range of IP addresses that users logging into the Appliance will be assigned. Usually 201-210 is ok. Again make sure that there are no computers on the Appliance network using the IP addresses in this range.
4. Select Apply.

From the remote computer:

1. From the start menu: Select Settings -> Network and Dial-up Connections -> Make a new connection.
2. Click Next on the wizard and select Connect to a private network through the internet. Click on Next.
3. Select Do not dial…..Click Next
4. Enter the host name. This should be a static IP if you have one. If not, then set up a DDNS account before continuing. This is where the Appliance can be found on the Internet. Click Next.
5. Select if you want to create this connection for all users on your remote network or just for the one computer. Click Next.

6. Name your connection and select if you want to have an icon on your desktop. Click Finish when done.
7. Use the user name and password on your Appliance to log in. You should be able to see the Appliance in your network neighborhood now. You must initiate the VPN connection each time unless you selected otherwise.

TIPS: If all you need is file transfer, we suggest using the FTP server feature, as it is faster and simpler. If you must use the PPTP VPN feature, then you can also disable the encryption under Properties -> Security to increase the performance.

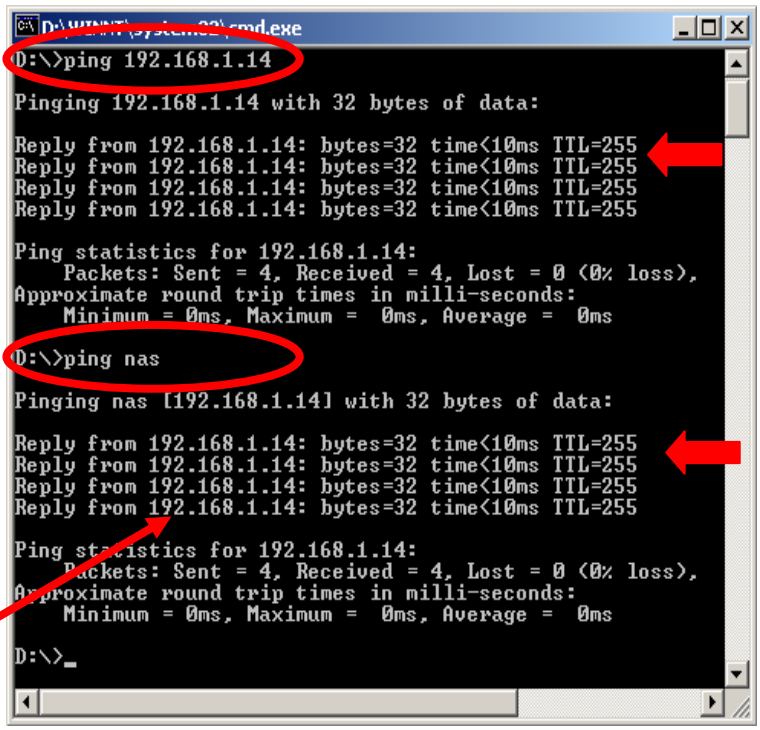
Pinging

You can test your network connection in various situations with this very simple method.

From a command prompt, type in: ping <IP address> or ping <network name>

If there are replies, then there is a connection running between the two machines.

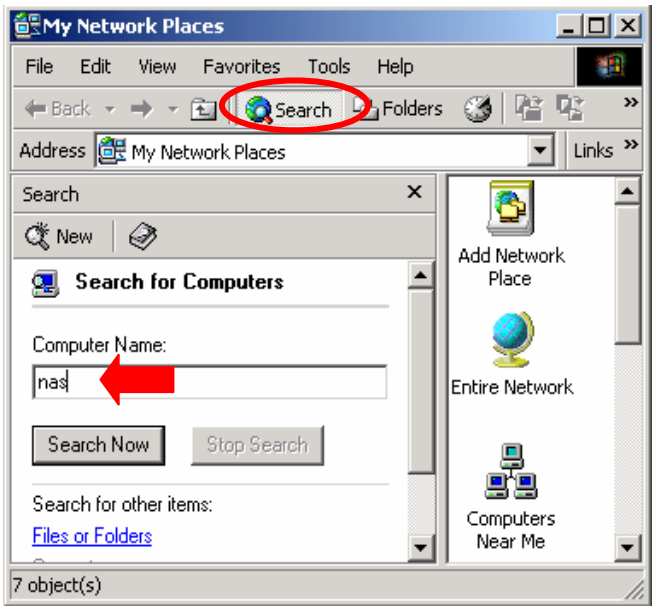
By pinging the device name, we also get the IP address of that device also.



Searching the Network for the NAS

If you are not able to locate the NAS in the **Network Neighborhood** or **My Network Places**, you can try to search for it.

Click **Search** under **My Network Places**.



Enter the name of the NAS or the Fixed IP address if configured that way and click **Search Now**.

All other company and/or products names are trademarks and/or registered trademarks of their respective owners.

AIRIS

www.airis.es